NPort Z3150 Series User's Manual

Second Edition, February 2015

www.moxa.com/product

© 2015 Moxa Inc. All rights reserved.

NPort Z3150 Series User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2015 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Introduction 1-1
Overview 1-2
Package Checklist 1-2
Product Features 1-2
Product Specifications 1-3

2. Getting Started 2-1
Overview 2-2
Panel Layout 2-2
LED Indicators 2-2
Top Panel LED Indicators 2-2
End Panel LED Indicators 2-3
Pull High/Low Resistors for RS-422/485 2-3
Function Block 2-4
Connecting the Hardware 2-4
Connecting to the Network 2-5
Connecting the Power 2-5
Connecting to a Serial Device 2-5

3. Initial IP Configuration 3-1
Overview 3-2
Factory Default IP Settings 3-2
Using ARP to Assign IP Address 3-2
Using the Telnet Console to Assign IP Address 3-3

4. Introduction to Operation Modes 4-1
Overview 4-2
Real COM Mode 4-2
TCP Server Mode 4-3
TCP Client Mode 4-3
UDP Mode 4-3

5. Web Console Configuration 5-1
Overview 5-2
Web Browser Settings 5-2
Navigating the Web Console 5-2
Quick Setup 5-3
Export/Import 5-5
Basic Settings 5-6
Server Name 5-6
Time Zone 5-6
Local Time 5-7
Time Server 5-7
Web Console 5-7
Telnet Console 5-8
Reset Button Protect 5-8
Network Settings 5-8
IP Configuration 5-9
IP Address 5-9
Netmask 5-9
Gateway 5-10
DNS Server 1 and 2 5-10
SNMP Settings 5-10
SNMPv1 5-10
Community name 5-10
Contact 5-11
Location 5-11
ZigBee Settings 5-11
PAN ID 5-11
Topology 5-11
Channel 5-12
Output Power 5-12
Advanced Settings 5-12
Start Byte 5-12
Security Settings 5-13
Encryption/Decryption 5-13
AES 128-bits Key 5-13
Serial Settings > Port 1 5-13
Port Alias 5-13
Baud Rate 5-14
Data Bits 5-14

Stop Bits 5-14
Parity 5-14
Flow Control 5-14
FIFO 5-14
Interface 5-15
Operating Settings > Port 1 or 2 5-15
Settings for RealCOM Mode 5-15
TCP Alive Check Time 5-16
Max Connection 5-16
Ignore Jammed IP 5-16
Allow Driver Control 5-17
Connection Goes Down 5-17
Packet Length 5-17
Delimiter 1 and 2 5-17
Delimiter Process 5-18
Force Transmit 5-18
Settings for TCP Server Mode 5-19
TCP Alive Check Time 5-19
Inactivity Time 5-19
Max Connection 5-20
Ignore Jammed IP 5-20
Allow Driver Control 5-20
TCP Port 5-20
Command Port 5-20
Packet Length 5-21
Delimiter 1 and 2 5-21
Delimiter Process 5-21
Force Transmit 5-22
Settings for TCP Client Mode 5-22
TCP Alive Check Time 5-23
Inactivity Time 5-23
Ignore Jammed IP 5-23
Destination Address 1 to 4 5-23
Designated Local Port 1 to 4 5-24
Connection Control 5-24
Packet Length 5-24
Delimiter 1 and 2 5-25
Delimiter Process 5-25
Force Transmit 5-25
Settings for UDP Mode 5-26
Destination Address 1 to 4 5-26
Local Listen Port 5-26
Packet Length 5-27
Delimiter 1 and 2 5-27
Delimiter Process 5-27
Force Transmit 5-28
UDP Multicast 5-28
Accessible IP Settings 5-29
Auto Warning Settings > E-mail and SNMP Trap > E-mail server 5-30
Mail Server 5-30
From E-mail Address 5-30
SNMP Trap Server IP 5-30
Auto Warning Settings > Event Settings 5-31
Firmware Upgrade 5-32
Change Password 5-33
Load Factory Default 5-33
Save/Restart 5-34

6. Web Console: Monitor 6-1

Overview 6-2
Monitor Line 6-2
Monitor Async 6-2
Monitor Async-Settings 6-3
Monitor ZigBee 6-3
Monitor ZigBee-Settings 6-4

7. Installing and Configuring the Software 7-1

Overview 7-2
NPort Windows Driver Manager 7-2
Installing NPort Windows Driver Manager 7-2
Adding Mapped Serial Ports 7-5
Configuring Mapped Serial Ports 7-8
NPort Search Utility 7-12

Installing NPort Search Utility 7-12
Finding NPort Device Servers on Network 7-14
Modifying NPort IP Addresses 7-15
Upgrading NPort Firmware 7-16
Linux Real TTY Drivers 7-17
Basic Steps 7-17
Installing Linux Real TTY Driver Files 7-17
Mapping TTY Ports 7-18
Removing Mapped TTY Ports 7-18
Removing Linux Driver Files 7-19
UNIX Fixed TTY Drivers 7-19
Installing the UNIX Driver 7-19
Configuring the UNIX Driver 7-20

A. SNMP Agents with MIB II & RS-232-Like Groups A-1
RFC1213 MIB-II Supported SNMP Variables A-2
System MIB A-2
Interfaces MIB A-2
IP MIB A-2
ICMP MIB A-2
UDP MIB A-2
Address Translation A-3
TCP MIB A-3
SNMP MIB A-3
RFC1317: RS-232 MIB Objects A-3
Generic RS-232-like Group A-3
RS-232-like General Port Table A-3
RS-232-like Asynchronous Port Group A-3
The Input Signal Table A-3
The Output Signal Table A-4

B. ZigBee Introduction B-1
Device Type B-2
Network Topology B-2

C. Well Known Port Numbers C-1

D. Federal Communication Commission Interference Statement D-1

E. FCC Warning Statement E-1

1

Introduction

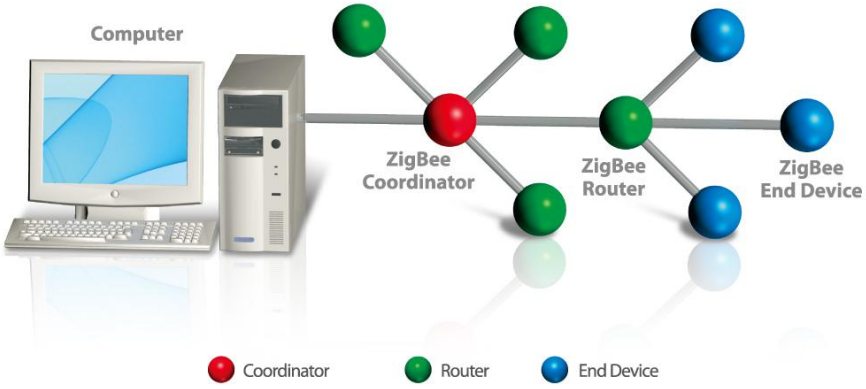
The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**

Overview

The NPort Z3150 is a gateway that provides computers with an Ethernet interface to a ZigBee PAN. Unlike a bridge, which logically extends a PAN across an Internet connection, a gateway provides network services on behalf of a ZigBee PAN. Software on any computer can control or monitor any ZigBee device in the PAN via the NPort Z3150.

The following architecture is the application overview of the NPort Z3150. The NPort Z3150 can only act as the ZigBee Coordinator (ZC). Thus, a converter such as the NPort Z2150 will be the ZigBee Router (ZR) and ZigBee End Device (ZED).



Package Checklist

Before installing the NPort Z3150, verify that the package contains the following items:

Standard Accessories

- NPort Z3150
- Document & Software CD
- RJ45 to RJ45 Ethernet cross-over cable
- Warranty statement
- Quick Installation Guide
- 2.4 GHz, omni-directional antenna

Optional Accessories

- DK-35A: DIN-rail mounting kit (35 mm)

NOTE: Please notify your sales representative if any of the above items are missing or damaged

Product Features

- Instant connection of any Ethernet device to a ZigBee network
- RS-232/422/485 port supporting baudrates up to 921.6 Kbps
- Web-based configuration over Ethernet
- Secure data access with AES
- Dual power inputs (1 power jack and 1 terminal block)

Product Specifications

ZigBee Interface
RF Standard: 802.15.4
Frequency Band: 2.4 GHz
Interface Immunity: DSSS
RF Data Rate: 250 Kbps
Rx sensitivity: -96 dBm
Tx Power: 4.5 dBm (Max)
Transmission Distance: Up tp 100m (in open areas)
Antenna: 2dB
PAN ID: 0x0000 – 0xFFFD
Node ID: 0 - 99
RF Channel: 11-26 (16 channels)
Device Type: Coordinator
Network Topology: Star, Mesh, Tree
Security: 128 bit AES encryption algorithms

Ethernet Interface
Number of Ports: 1
Speed: 10/100 Mbps, auto MDI/MDIX
Connector: RJ45
Magnetic Isolation Protection: 1.5 KV built-in

Serial Interface
Number of Port: 1
Serial Standards: RS-232/422/485
Connector: DB9 male
RS- 485 Data Direction Control: ADDC (Automatic Data Direction Control)

Serial Communication Parameters
Data Bits: 5, 6, 7, 8
Stop Bits: 1, 1.5, 2
Parity: None, Even, Odd, Space, Mark
Flow Control: RTS/CTS, XON/XOFF, DTR/DSR
Baudrate: 50 bps to 921.6Kbps

Serial Signals
RS-232: TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND
RS-422: TxD+, TxD-, RxD+, RxD-, GND
RS-485-4w: TxD+, TxD-, RxD+, RxD-, GND
RS-485-2w: Data+, Data-, GND

Software
Configuration Method: Web Console
Firmware Upgrade: Web Console or Search Utility

Hardware
DIP Switch: (inside the box):
- SW1/2: Pull high/low resister
- SW3: Termination for RS-422/485

Reset Button: Reset to default

Physical Characteristics
Weight: 380g
Dimension:
- Without ears: 67 x 100.4 x 22 mm (2.64 x 3.95 x 0.87 in)
- With ears: 90 x 100 x 22 mm (3.54 x 3.94 x 0.87 in)

Environmental Limits

Operating Temperature:

Standard Models: 0 to 55°C (32 to 131°F)

Wide Temp. Models: -40 to 75°C (-40 to 167°F)

Operating Humidity: 5 to 95% RH

Storage Temperature: -40 to 85°C (-40 to 185°F)

Power Requirements

Input Voltage: 12 to 48 VDC

Power Consumption: 120 mA @ 12 V

Connector: Power jack and terminal block

Regulatory Approvals

EMC: CE (EN55022 Class A, EN55024), FCC Part 15 Subpart B Class A

Safety: UL (UL60950-1), LVD (EN60950-1)

Reliability

Automatic Reboot Trigger: Built-in WDT (watchdog timer)

MTBF (meantime between failures): 1109589 hrs

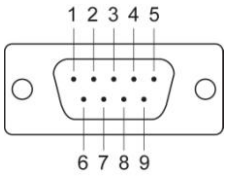
Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

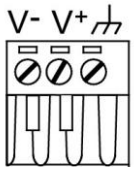
Pin Assignments and Cable Wiring

PIN	RS-232	RS-422, 4w RS-485	2w RS-485
1	DCD	TxD-(A)	–
2	RXD	TxD+(B)	–
3	TXD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	–	–	–



Power Input Pinouts

	V+	V-
Shielded Ground	DC Power Input 1	DC Power Input 1



2

Getting Started

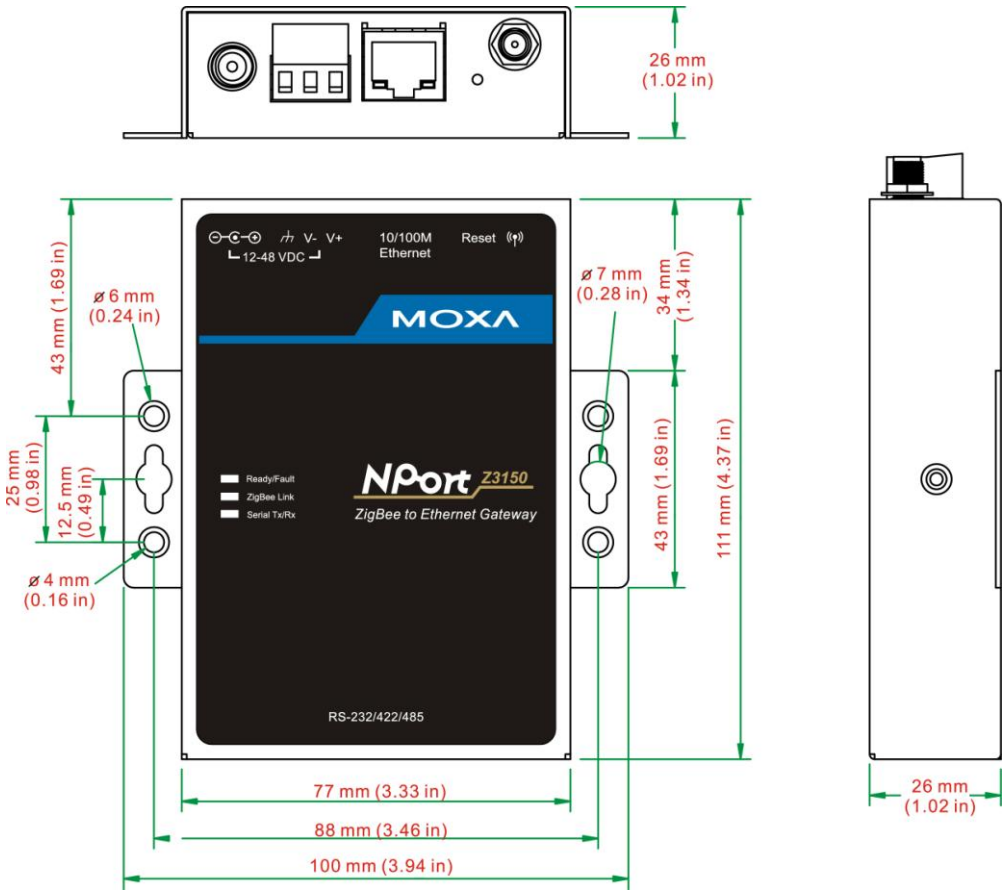
The following topics are covered in this chapter:

- **Overview**
- **Panel Layout**
- **LED Indicators**
  - Top Panel LED Indicators
  - End Panel LED Indicators
- **Pull High/Low Resistors for RS-422/485**
- **Function Block**
- **Connecting the Hardware**
  - Connecting to the Network
  - Connecting the Power
  - Connecting to a Serial Device

Overview

This chapter presents the hardware features of the NPort Z3150 and explains how to connect the hardware.

Panel Layout



LED Indicators

Top Panel LED Indicators

There are three LEDs on NPort Z3150.

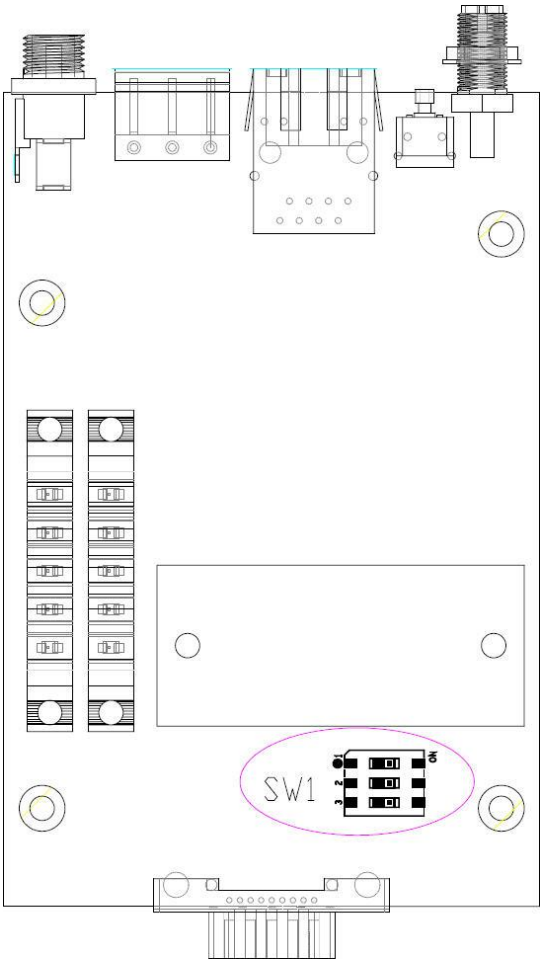
LED Name	LED Color	Descriptions
Ready	Green	On: System power on Blinking: 1) Device locating 2) Pull down the reset button
Fault	Red	On: System initialization failed
ZigBee	Green	On: ZigBee initialized/PAN connection normal
		Blinking: ZigBee Tx/Rx
		Off: ZigBee initial/PAN connection failure
Serial Tx	Green	Serial data output to serial port
Serial Rx	Orange	Serial data input from serial port

End Panel LED Indicators

Name	Color	Function
Ethernet	Orange	10 Mbps Ethernet connection
	Green	100 Mbps Ethernet connection
	Off	Ethernet cable is disconnected or has a short

Pull High/Low Resistors for RS-422/485

You may need to set the pull high/low resistors when termination resistors are used for certain RS-422 or RS-485 environments.

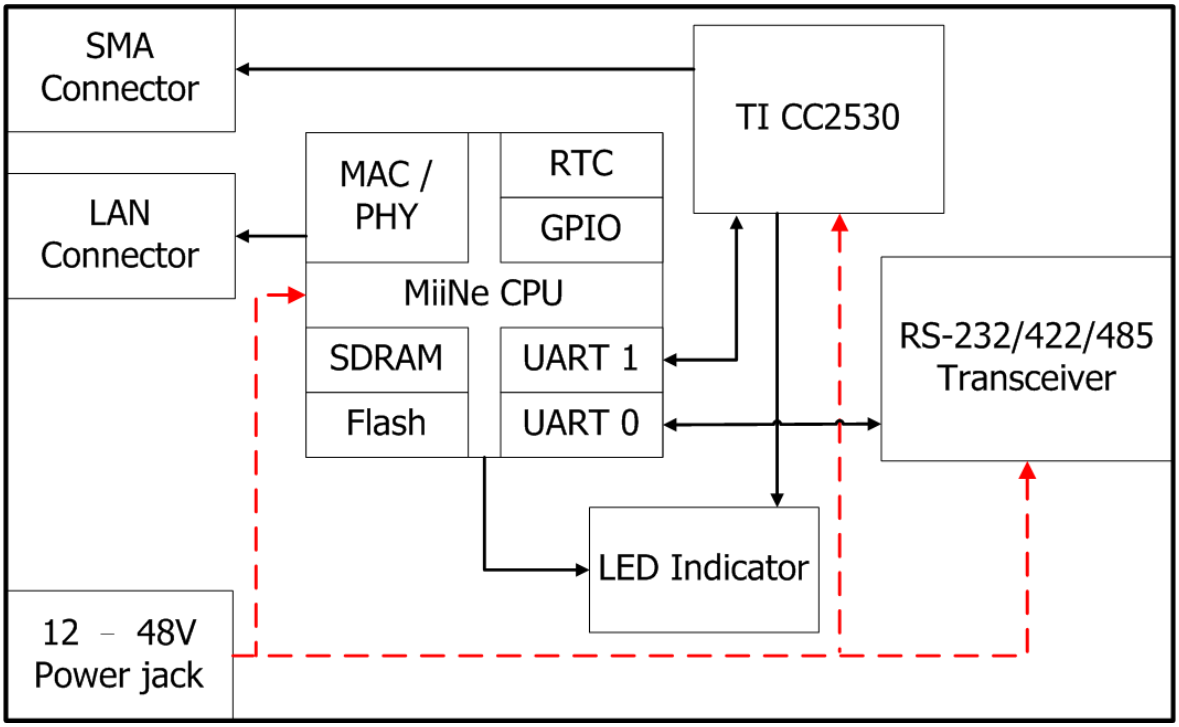


	SW	1	2	3
		Pull High	Pull Low	Terminator
	ON	1KΩ	1KΩ	120Ω
Default	OFF	150KΩ	150KΩ	---

ATTENTION

Do not use the 1 KΩ setting while in RS-232 mode. Doing so will degrade the RS-232 signals and reduce the effective communication distance.

Function Block



Connecting the Hardware

ATTENTION

Before connecting the hardware, follow these important wiring safety precautions:

Disconnect power source

Do not install or wire this unit or any attached devices with the power connected. Disconnect the power before installation by removing the power cord before installing and/or wiring your unit.

Follow maximum current ratings

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Use caution - unit may get hot

The unit will generate heat during operation, and the casing may feel hot to the touch. Take care when handling unit. Be sure to leave adequate space for ventilation.

The following guidelines will help ensure trouble-free signal communication with the NPort.

- Use separate paths to route wiring for power and devices to avoid interference. Do not run signal or communication wiring and power wiring in the same wire conduit. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
- Keep input wiring and output wiring separate.
- Label all wiring to each device in the system for easier testing and troubleshooting

Connecting to the Network

Use the supplied Ethernet cable to connect the NPort to your Ethernet network. If the cable is properly connected, the NPort will indicate a valid connection to the Ethernet as follows:

- A green Ethernet LED indicates a valid connection to a 100 Mbps Ethernet network.
- An orange Ethernet LED indicates a valid connection to a 10 Mbps Ethernet network.
- A flashing Ethernet LED indicates that Ethernet packets are being transmitted or received.

Connecting the Power

Connect the VDC power line (12 to 48 V) to the NPort's power jack or terminal block. If power is properly connected, the "Ready" LED will initially glow red. When the system is ready, the "Ready" LED will turn green.

Connecting to a Serial Device

Use a serial cable to connect your serial device to a serial port on the NPort.

3

Initial IP Configuration

The following topics are covered in this chapter:

- **Overview**
- **Factory Default IP Settings**
- **Using ARP to Assign IP Address**
- **Using the Telnet Console to Assign IP Address**

Overview

This chapter presents several ways to assign the NPort's IP address for the first time. Please refer to Chapter 2 for instructions on connecting to the network.

The web console is the recommended method for configuring the NPort. Please refer to Chapter 5 and 6 for details on using the web console for configuration.

Factory Default IP Settings

Network Interface	IP Configuration	IP Address	Netmask
LAN	Static	192.168.127.254	255.255.255.0

If your NPort is configured to obtain its IP settings from a DHCP or BOOTP server but is unable to get a response, it will use the factory default IP address and netmask.

ATTENTION

If you forget the IP address of your NPort, you can look it up using the NPort Search Utility. After NPort Search Utility has found all NPorts on the network, each unit will be listed with its IP address. Please refer to Chapter 7 for additional information on using NPort Search Utility.

Using ARP to Assign IP Address

The ARP (Address Resolution Protocol) command can be used to assign an IP address to the NPort. The ARP command tells your computer to associate the NPort's MAC address with the specified IP address. You must then use Telnet to access the NPort, at which point the device server's IP address will be reconfigured. This method only works when the NPort is configured with default IP settings.

Select a valid IP address for your NPort. Consult with your network administrator if necessary.
Obtain the NPort's MAC address from the label on its bottom panel.

From the DOS prompt, execute the **arp -s** command with the desired IP address and the NPort's MAC address, as in the following example:

arp -s 192.168.200.100 00-90-E8-xx-xx-xx

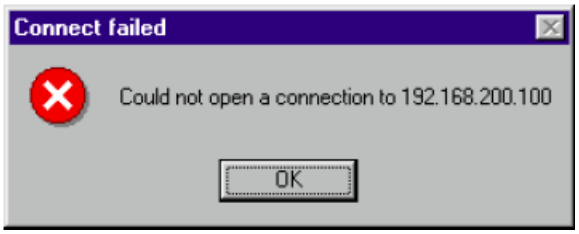
In this example 192.168.200.100 is the new IP address that will be assigned to the NPort, and 00-90-E8-xx-xx-xx is the NPort's MAC address.

From the DOS prompt, execute a special Telnet command using port 6000, as in the following example:

telnet 192.168.200.100 6000

In this example, 192.168.200.100 is the new IP address that will be assigned to the NPort.

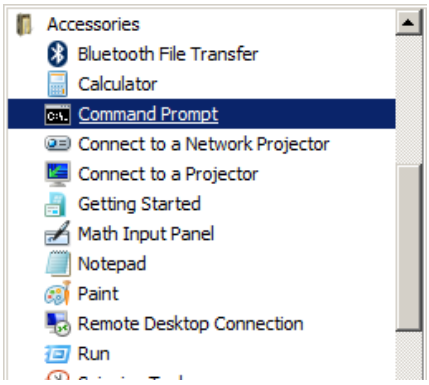
You should see a message indicating that the connection failed.



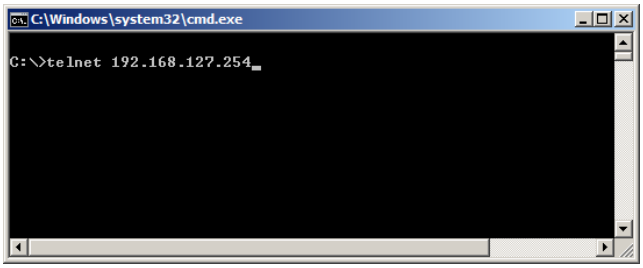
The NPort will automatically reboot with the new IP address. You can verify that the configuration was successful by connecting to the new IP address with Telnet, ping, the web console, or NPort Search Utility.

Using the Telnet Console to Assign IP Address

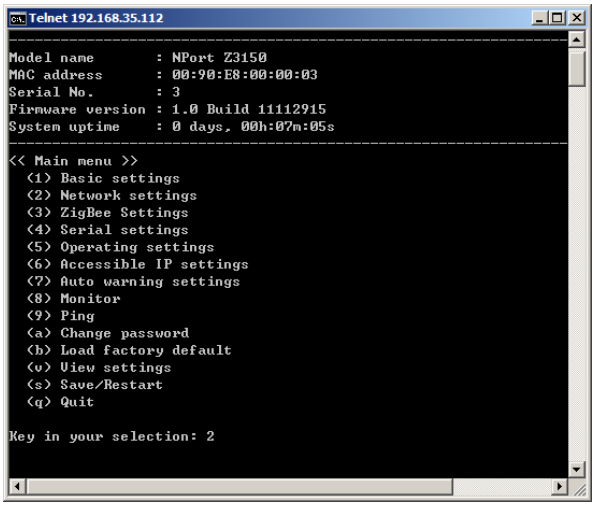
1. Select **Command Prompt** from **Accessories**



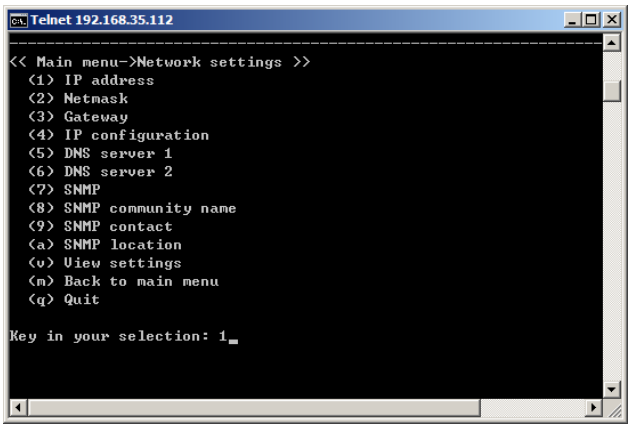
2. Enter **telnet 192.168.127.254** (the NPort's default IP address) and click **[OK]**.



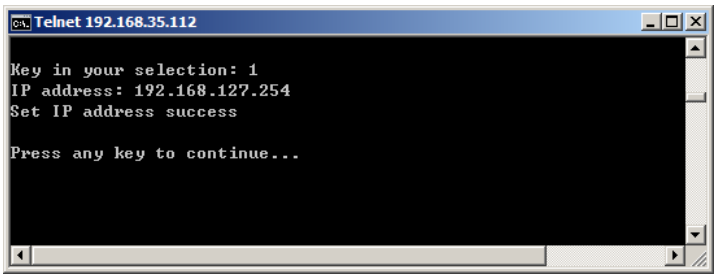
3. Select 2 to select Network settings and press Enter



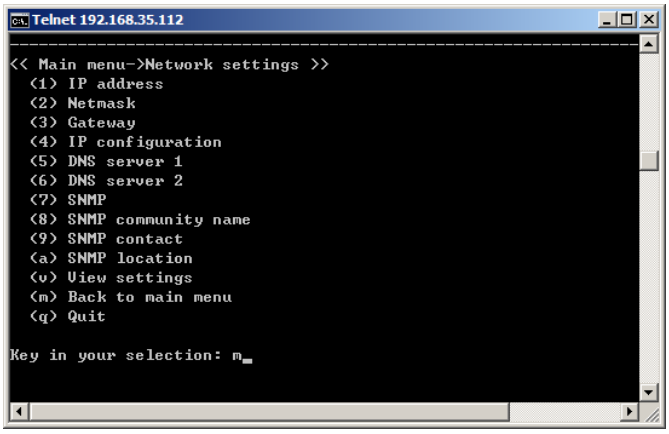
4. Input 1 to select IP address and press Enter



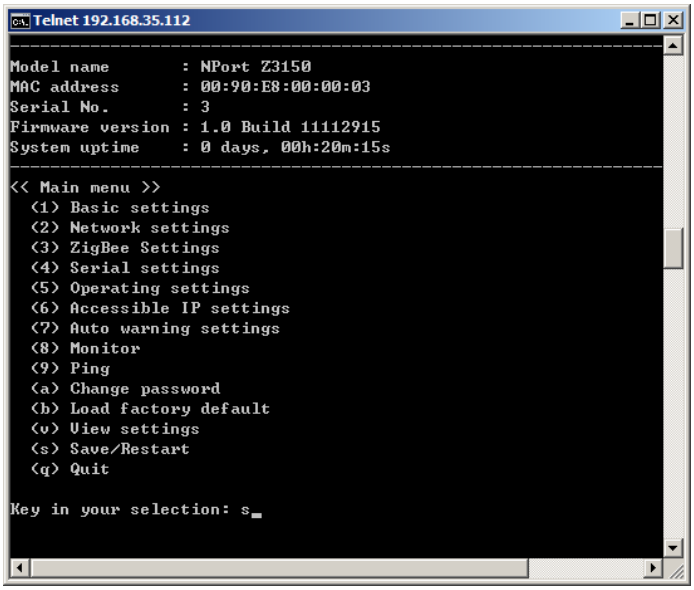
5. Key in your desired IP address and press Enter



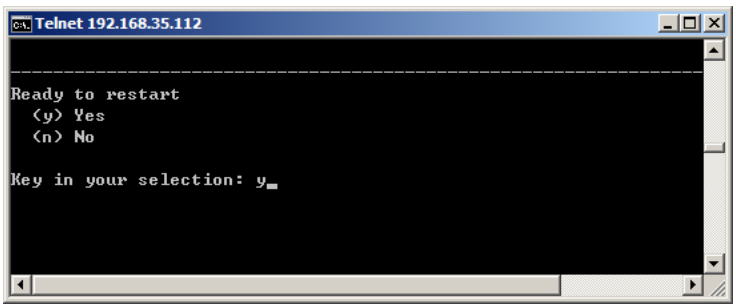
6. Input m to go back main menu and press Enter



7. Input s to save and restart configuration and press Enter



8. Press y to confirm action for save and restart configuration and press Enter. The NPort will reboot with the new IP settings.



4

Introduction to Operation Modes

The following topics are covered in this chapter:

- **Overview**
- **Real COM Mode**
- **TCP Server Mode**
- **TCP Client Mode**
- **UDP Mode**

Overview

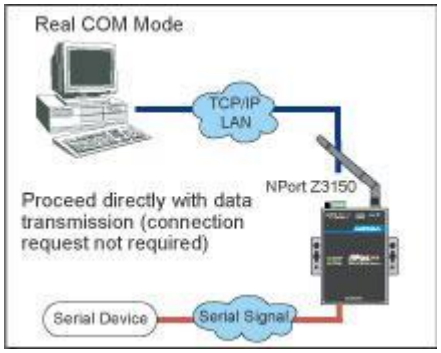
This chapter introduces the different serial port operation modes that are available on the NPort Z3150. Each serial port on the NPort is configured independently of the other ports, with its own serial communication parameters and operation mode. The serial port's operation mode determines how it interacts with the network, and different modes are available to encompass a wide variety of applications and devices.

Real COM mode allows serial-based software to access the NPort serial port as if it were a local serial port on a PC. This mode is appropriate when your application relies on Windows or Linux software that was originally designed for locally attached COM or TTY devices. With this mode, you can access your devices from the network using your existing COM/TTY-based software, without investing in additional software.

Three different socket modes are available for user-developed socket programs: **TCP Server**, **TCP Client**, and **UDP Server/Client**. For TCP applications, the appropriate mode depends on whether the connection will be hosted or initiated from the NPort serial port or from the network. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer speedier delivery. UDP also allows multicasting of data to groups of IP addresses and would be suitable for streaming media or non-critical messaging applications such as LED message boards.

Real COM Mode

Real COM mode is designed to work with NPort drivers that are installed on a network host. COM drivers are provided for Windows systems, and TTY drivers are provided for Linux and UNIX systems. The driver establishes a transparent connection to the attached serial device by mapping a local serial port to the NPort serial port. Real COM mode supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.



ATTENTION

Real COM drivers are installed and configured through NPort Windows Driver Manager.

Real COM mode allows you to continue using your serial communications software to access devices that are now attached to your NPort device server. On the host, the NPort Real COM driver automatically intercepts data sent to the COM port, packs it into a TCP/IP packet, and redirects it to the network. At the other end of the connection, the NPort device server accepts the Ethernet frame, unpacks the TCP/IP packet, and sends the serial data to the appropriate device.

ATTENTION

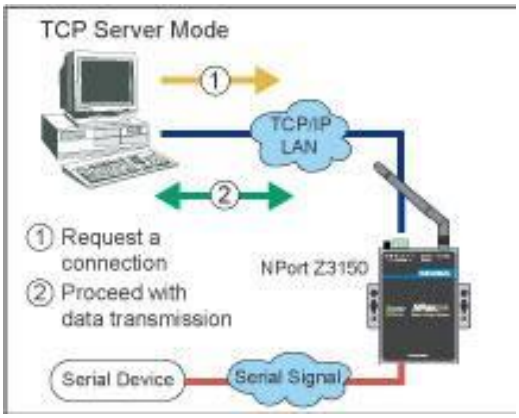
In Real COM mode, several hosts can have simultaneous access control over the NPort serial port. If necessary, you can limit access by using the NPort's Accessible IP settings. Please refer to Chapter 5 for additional information on Accessible IP settings.

TCP Server Mode

In TCP Server mode, the NPort serial port is assigned an IP:port address that is unique on your TCP/IP network. It waits for the host computer to establish a connection to the attached serial device. This operation mode also supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

Data transmission proceeds as follows:

1. A host requests a connection to the NPort serial port.
2. Once the connection is established, data can be transmitted in both directions—from the host to the device, and from the device to the host.

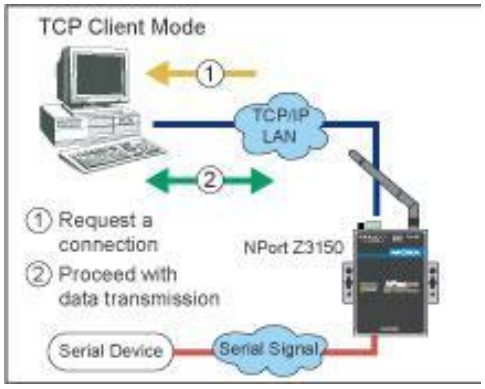


TCP Client Mode

In TCP Client mode, the NPort actively establishes a TCP connection to a specific network host when data is received from the attached serial device. After the data has been transferred, the NPort can automatically disconnect from the host computer through the **Inactivity time** settings. Please refer to Chapter 7 for details on these parameters.

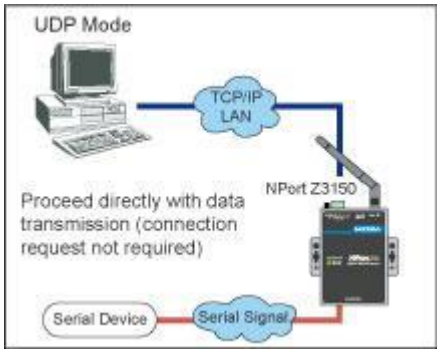
Data transmission proceeds as follows:

1. The NPort requests a connection from the host.
2. The connection is established and data can be transmitted in both directions between the host and device.



UDP Mode

UDP is similar to TCP but is faster and more efficient. Data can be broadcast to or received from multiple network hosts. However, UDP does not support verification of data and would not be suitable for applications where data integrity is critical. It is ideal for message display applications.



5

Web Console Configuration

The Web Console is the most user-friendly method available to configure NPort Z3150. In this chapter, we introduce the Web Console function groups and function definitions.

The following topics are covered in this chapter:

- **Overview**
- **Quick Setup**
- **Export/Import**
- **Basic Settings**
- **Network Settings**
- **SNMP Settings**
- **ZigBee Settings**
- **Security Settings**
- **Serial Settings > Port 1**
- **Operating Settings > Port 1 or 2**
- **Settings for RealCOM Mode**
- **Settings for TCP Server Mode**
- **Settings for TCP Client Mode**
- **Settings for UDP Mode**
- **UDP Multicast**
- **Accessible IP Settings**
- **Auto Warning Settings > E-mail and SNMP Trap > E-mail server**
- **Auto Warning Settings > Event Settings**
- **Firmware Upgrade**
- **Change Password**
- **Load Factory Default**
- **Save/Restart**

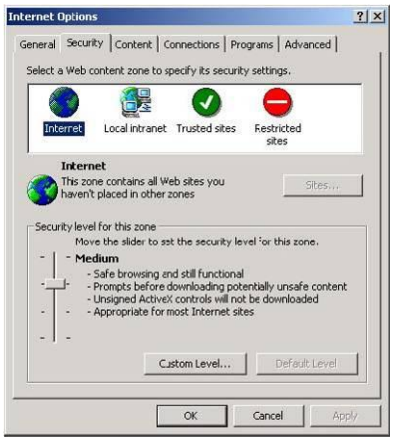
Overview

This chapter introduces the NPort Web Console and explains how to configure the basic settings.

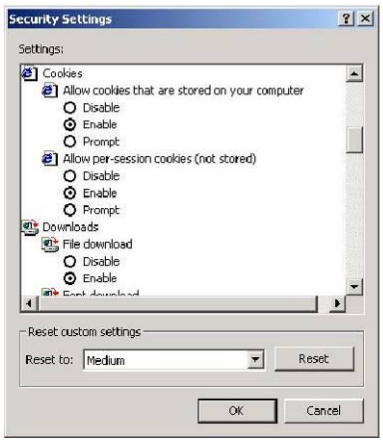
The NPort can be configured from anywhere on the network through its Web Console. Simply point the browser to the device server's IP address to open the web console. Network settings, operation mode, and other items can all be configured through the browser.

Web Browser Settings

In order to use the web console, you will need to have cookies enabled for your browser. Please note that the web console uses cookies only for password transmission. For Internet Explorer, cookies can be enabled by right-clicking the Internet Explorer icon on your desktop and selecting Properties from the context menu.



On the Security tab, click "Custom Level…" and enable these two items:
Allow cookies that are stored on your computer.
Allow per-session cookies (not stored).



ATTENTION

If you are not using Internet Explorer, cookies are usually enabled through a web browser setting such as "allow cookies that are stored on your computer" or "allow per-session cookies."

Navigating the Web Console

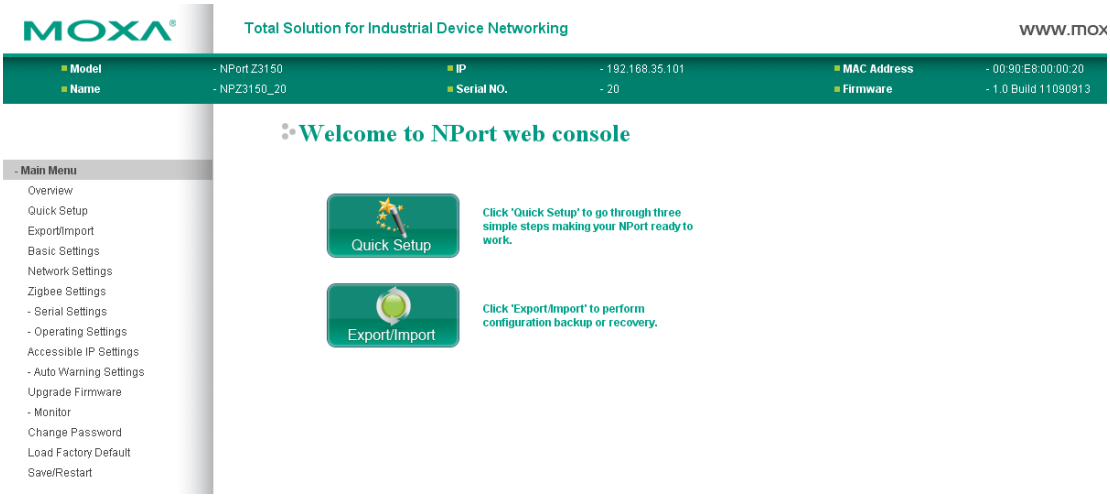
To open the web console, enter your device server's IP address in the website address line. If you are configuring the NPort for the first time over an Ethernet cable, you will use the default IP address, **192.168.127.254**.

If prompted, enter the console password. You will only be prompted for a password if you have enabled password protection on the device server. The password will be transmitted with MD5 encryption over the Ethernet.

ATTENTION

If you have forgotten the password, you can use the reset button to load factory defaults, but this will erase all previous configuration information.

The web console will appear as shown below.



Settings are presented on pages that are organized by folder. Select the desired folder in the left navigation panel to open that page. The page will be displayed in the main window on the right. Certain folders can be expanded by clicking the adjacent "-" symbol.

For example, if you click **Serial Settings** in the navigation panel, the main window will show a page of basic settings that you can configure.

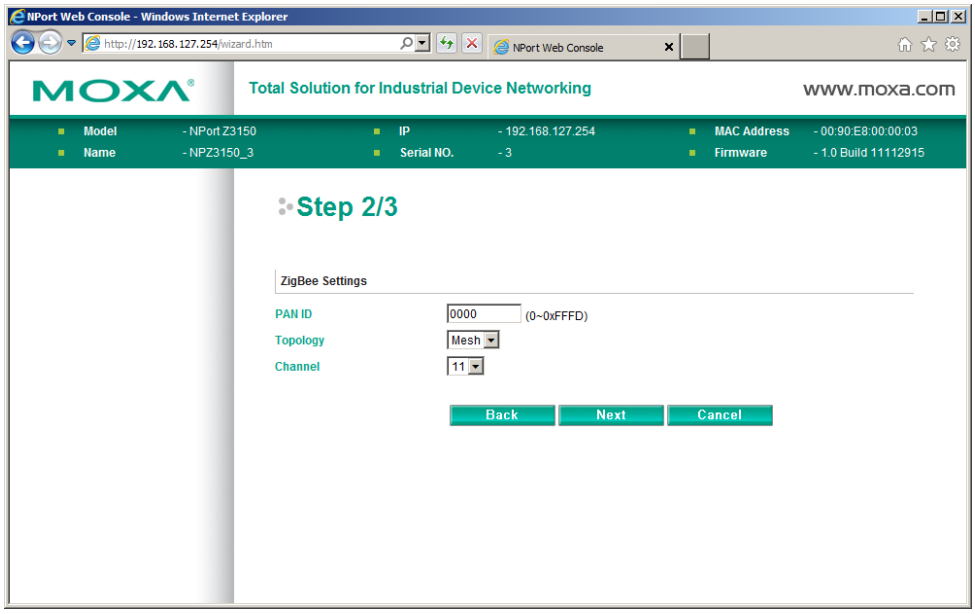
After you have made changes on a page, you must click **[Submit]** in the main window before jumping to another page. Your changes will be lost if you do not click **[Submit]**.

After you have finished modifying the desired pages, you must save and restart the device server for the new settings to take effect. You may complete this in one step by clicking **[Save/Restart]** after you submit a change. Changes will not take effect until they are saved and the NPort is restarted. If you restart the NPort without saving your configuration, all configuration changes will be lost.

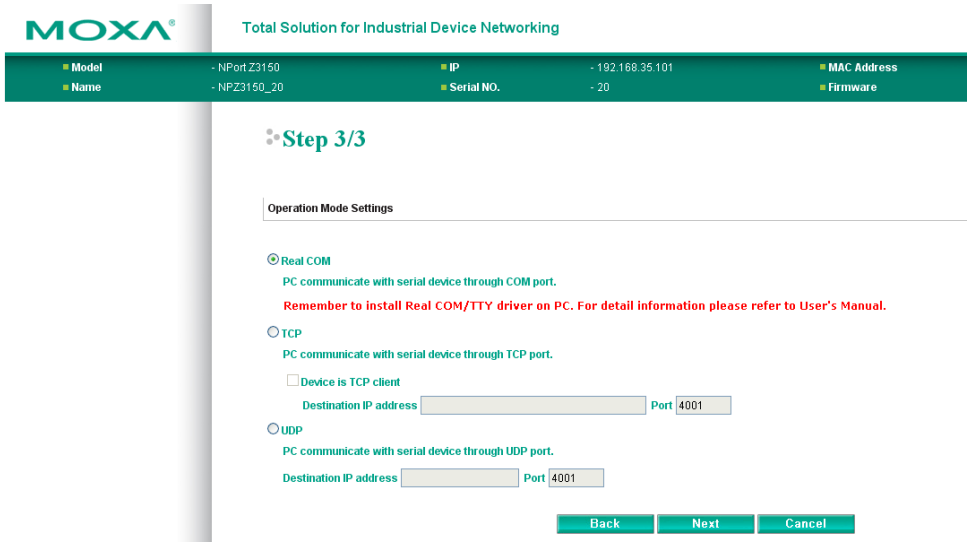
Quick Setup

Quick Setup streamlines configuration of your NPort into three basic and quick steps that covers the most commonly-used settings. At any time while in Quick Setup you may click the **Back** button to return to the previous step, or the **Cancel** button to reverse all settings. For more detailed settings, please refer to the "Basic Settings," "Network Settings," "ZigBee Settings," and "Operating Settings" sections later in this chapter.

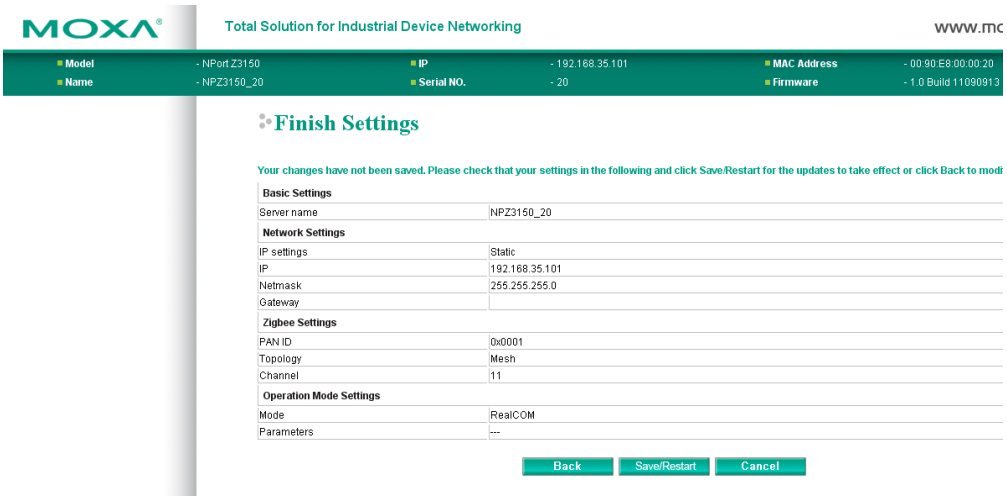
In Step 1/3, you must assign a valid IP address to the NPort Z3150 before it will work in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. In addition, the server name field is a useful way to specify the location or application of different NPort Z3150s.



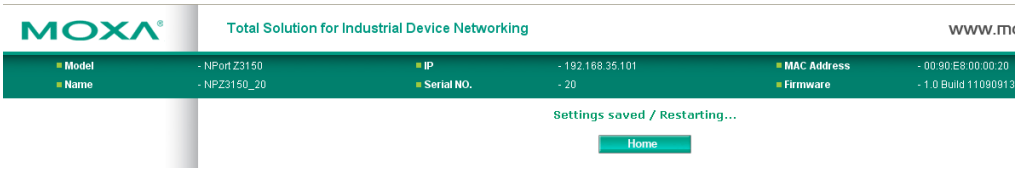
In the Step 2/3, you can modify the ZigBee settings.



In the Step 3/3, you must specify which operation mode you will use.



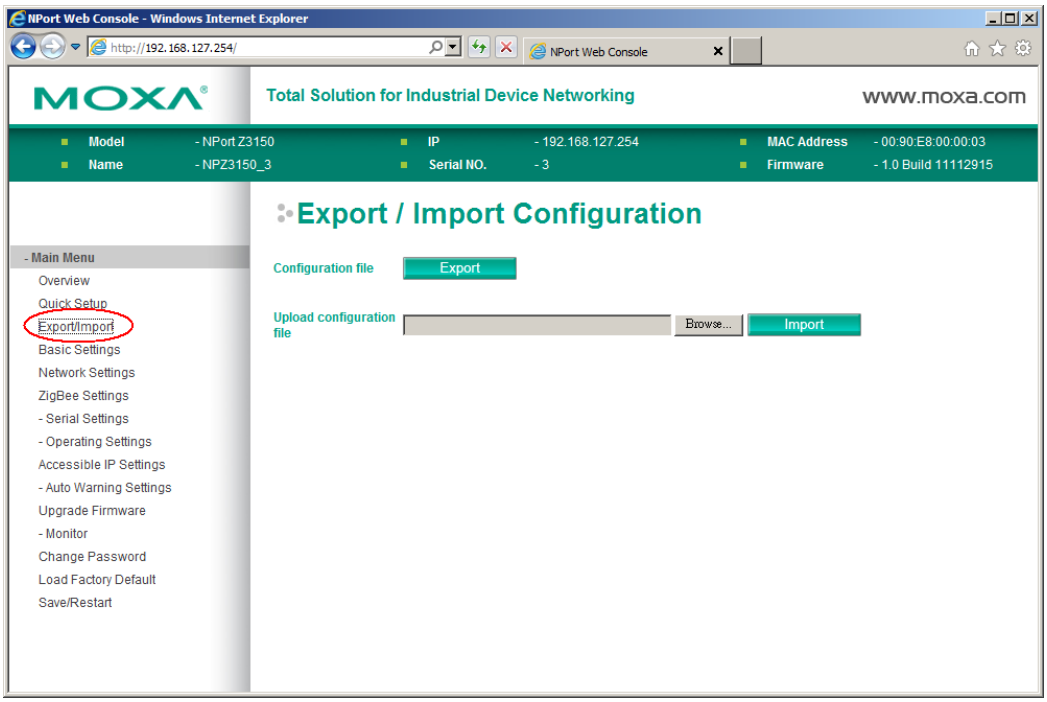
Review your settings at the **Finish Settings** page to confirm that they are correct, and then click the **Save/Restart** button to restart the device with the new settings.



Note that if you changed the IP address, you will not be able to return to the Home Page with the **Home** button.

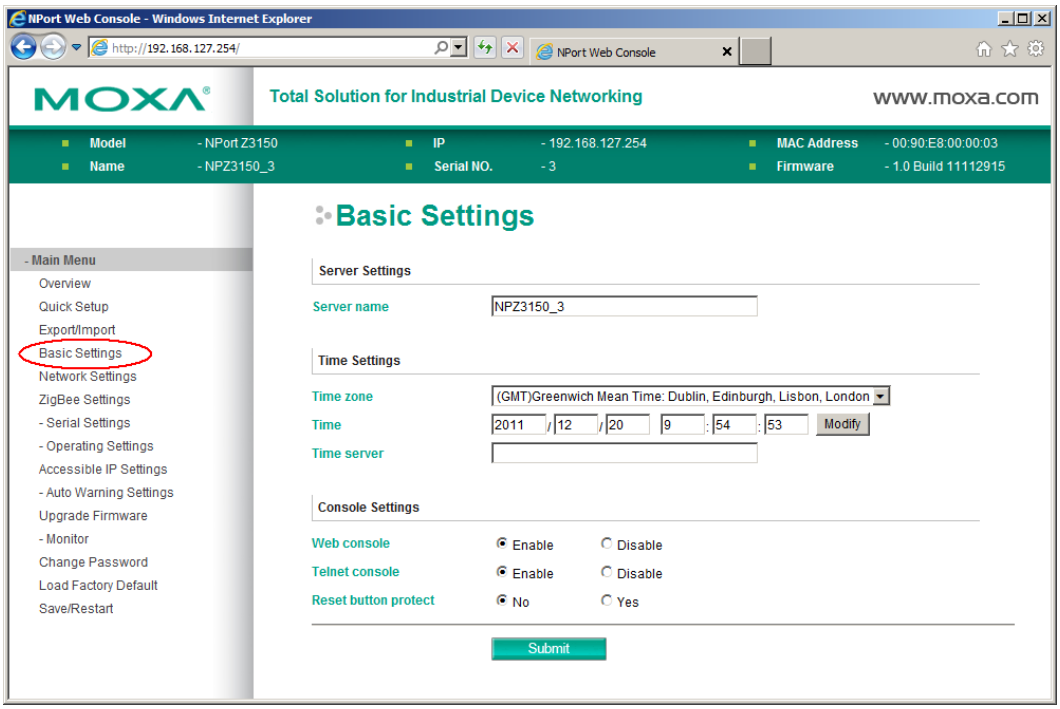
Export/Import

Export/Import allows you to back up and recover your settings.



Click **Export**, to store all configuration data into a default file, **<Servername>.txt**. Click the **Import** button to upload a configuration file to the NPort Z3150.

Basic Settings



On the **Basic Settings** page, you can configure **Server name**, **Server location**, **Time zone (24-hour)**, **Local time**, **Time server**, and **Console** Settings.

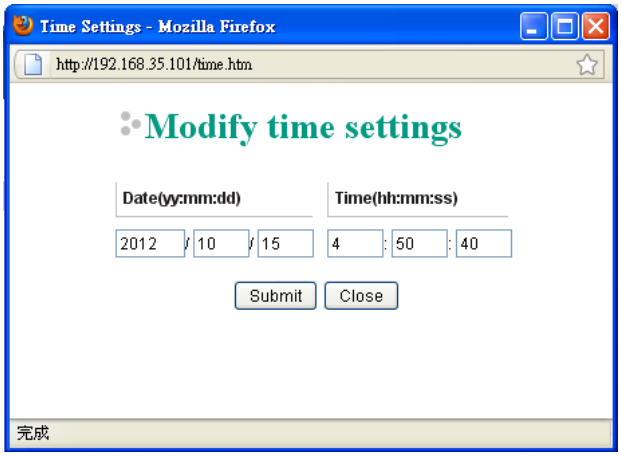
Server Name

Default	NPZ3150_<serial no.>
Options	free text (e.g., "Server 1")
Description	This is an optional free text field to help you differentiate one device server from another. It does not affect operation of the NPort device server.

Time Zone

Default	(GMT)Greenwich Mean Time
Options	(GMT)Greenwich Mean Time (GMT-01:00)Azores, Cape Verde Is. (GMT-02:00)Mid-Atlantic etc.
Description	This field shows the currently selected time zone and allows you to select a different time zone.

Local Time

Default	
Options	Date (yy:mm:dd), Time (hh:mm:ss)
Description	The NPort has a built-in real-time clock that allows you to add time information to functions such as the automatic warning e-mail or SNMP trap. This field shows the current time according to the NPort's built-in real-time clock. This is not a live field, so you will need to refresh the browser to get an updated reading. Click **[Modify]** to adjust the real-time clock. Make sure that you first select the correct time zone. The real-time clock will be updated immediately, with no need to restart the NPort. 

ATTENTION

There is a risk of explosion if the real-time clock battery is replaced incorrectly!

The real time clock is powered by a lithium battery. We strongly recommend that you obtain assistance from a Moxa support engineer before replacing the battery. Please contact the Moxa RMA service team if you need to change the battery.

Time Server

Default	
Options	IP address or domain name (e.g., "192.168.1.1" or "time.nist.gov")
Description	This optional field specifies your time server's IP address or domain name, if a time server is used in your network. The NPort supports SNTP (RFC-1769) for automatic time calibration. The device server will request time information from the specified time server every 10 minutes.

Web Console

Default	Enable
Options	Enable or Disable
Description	The "Disable" option for "Web Console" is included for security reasons. In some cases, you may want to disable one or both of these console utilities as an extra precaution to prevent unauthorized users from accessing your NPort Z3150. The factory default for Web console is Enable.

Telnet Console

Default	Enable
Options	Enable or Disable
Description	The "Disable" option for "Telnet Console" is included for security reasons. In some cases, you may want to disable one or both of these console utilities as an extra precaution to prevent unauthorized users from accessing your NPort Z3150. The factory default for Telnet console is Enable.

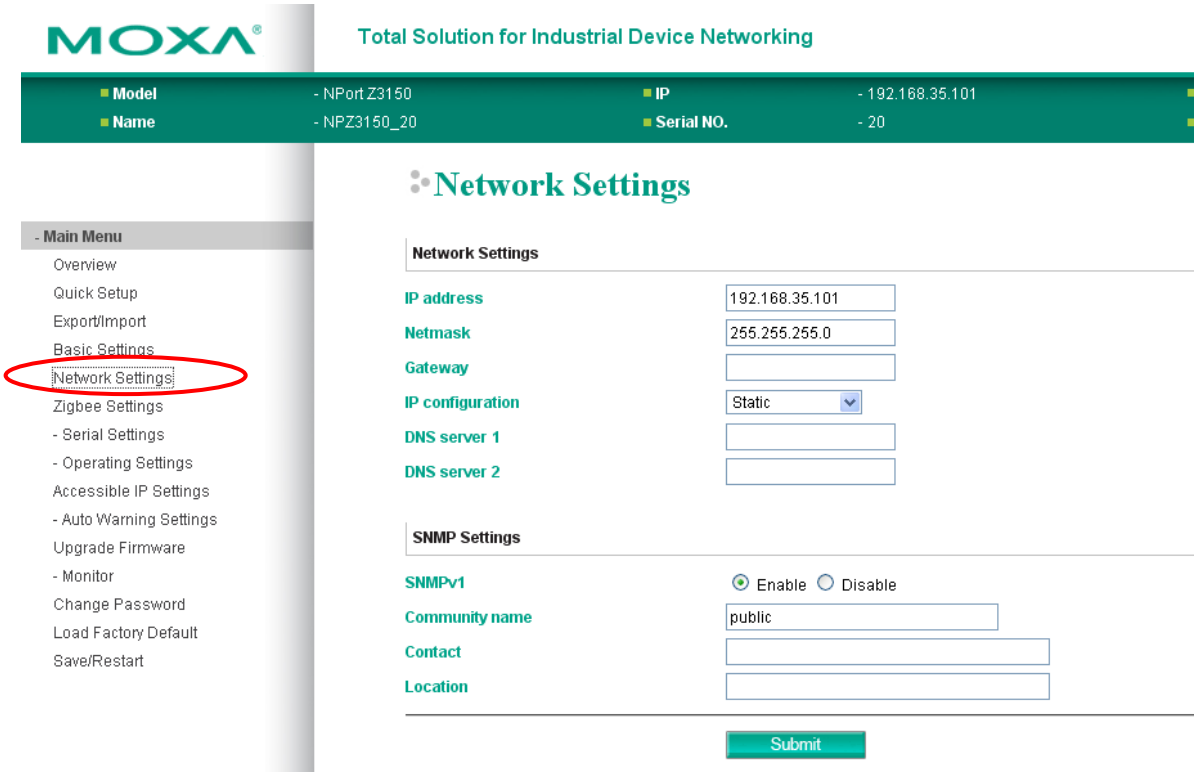
ATTENTION

If you disable both the "Web console" and "Telnet console," you can still use NPort Administrator to configure NPort Z3150 device servers either locally or remotely over the network. Refer to Chapter 7 for more details.

Reset Button Protect

Default	No
Options	Yes or No
Description	Select the **Yes** option to allow limited use of the Reset Button. In this case, the Reset Button can be used for only 60 seconds. I.e., 60 seconds after booting up, the Reset Button will be disabled automatically.

Network Settings



You can modify **IP configuration**, **IP address**, **Netmask**, **Gateway**, **Speed**, and **SNMP** settings.

You must assign a valid IP address to the NPort before it will work in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. The IP address must be unique within the network; otherwise the NPort will not have a valid connection to the network. First-time users should refer to Chapter 3, "Initial IP Address Configuration," for more information.

IP Configuration

Default	Static
Options	Static, DHCP, DHCP/BOOTP, BOOTP
Description	This field determines how the NPort's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

ATTENTION

In Dynamic IP environments, the firmware will retry 3 times every 30 seconds until network settings are assigned by the DHCP or BOOTP server. The Timeout for each try increases from 1 second, to 3 seconds, to 5 seconds.
If the DHCP/BOOTP Server is unavailable, the firmware will use the default IP address (192.168.127.254), Netmask, and Gateway for IP settings.

IP Address

Default	192.168.127.254
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address that will be assigned to your NPort device server. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment. If your device server will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

Netmask

Default	255.255.255.0
Options	Netmask setting (e.g., "255.255.0.0")
Description	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort device server will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the device server, a connection is established directly from the device server. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

Gateway

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort device server needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

DNS Server 1 and 2

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the DNS server's IP address, if applicable. With the DNS server configured, the NPort device server can use domain names instead of IP addresses to access hosts. Domain Name System (DNS) is how Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, that it is usually easier to remember than the numeric IP address. A DNS server is a host that translates a text-based domain name into an IP address in order to establish a TCP/IP connection. When the user wants to visit a particular website, the user's computer sends the domain name (e.g., www.moxa.com) to a DNS server to request that website's numeric IP address. When the IP address is received from the DNS server, the user's computer uses that information to connect to the website's web server. The NPort will play the role of a DNS client, actively querying the DNS server for the IP address associated with a particular domain name.

SNMP Settings

SNMPv1

Default	Enable
Options	Enable or Disable
Description	Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. NPort Z3150 supports SNMP version 1. In some cases, you can disable this function.

Community name

Default	public
Options	free text, 1 to 39 characters (e.g., "private")
Description	A community name is a plain-text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

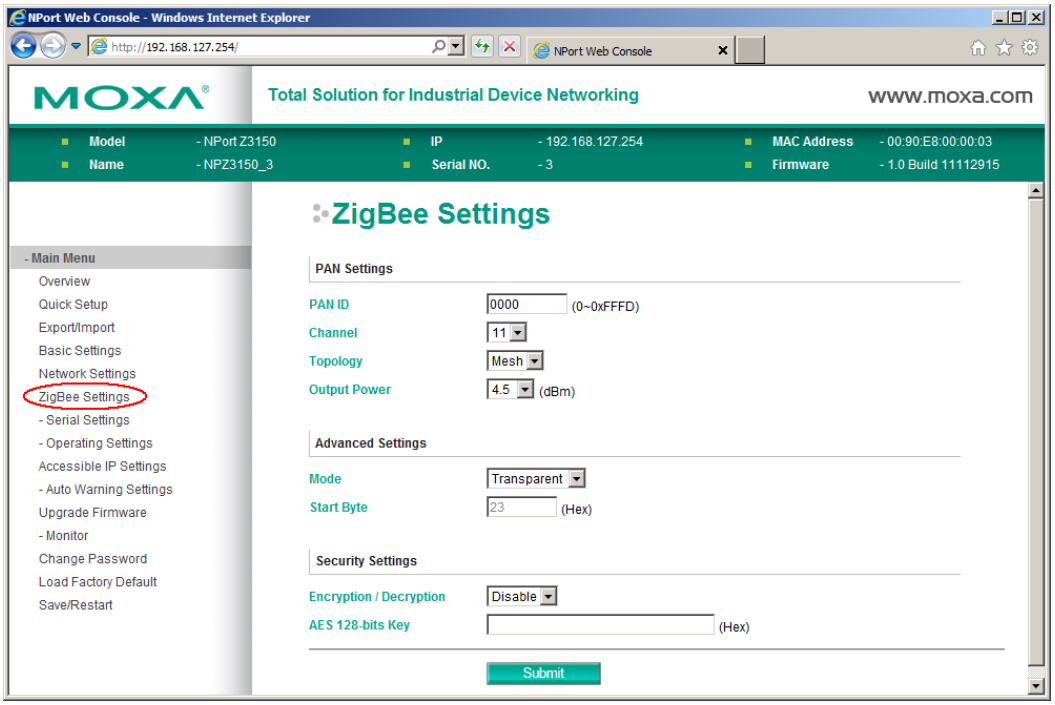
Contact

Default	
Options	free text, 1 to 39 characters (E.g., Support, 886-89191230 #300)
Description	The SNMP contact information usually includes an emergency contact name and telephone or pager number.

Location

Default	
Options	free text, 1 to 39 characters (E.g., Floor 1, office 2)
Description	Specify the location string for SNMP agents such as NPort Z3150. This string is usually set to the street address where the NPort Z3150 is physically located.

ZigBee Settings



On the **ZigBee** page is used to modify ZigBee settings, such as PAN ID, Channel and Topology.

PAN ID

Default	0000
Options	0 to 0xFFFD (Hex)
Description	The PAN identifier.

Topology

Default	Mesh
Options	Star, Tree and Mesh
Description	Network topology, supports three kinds of topology: Star, Tree and Mesh.

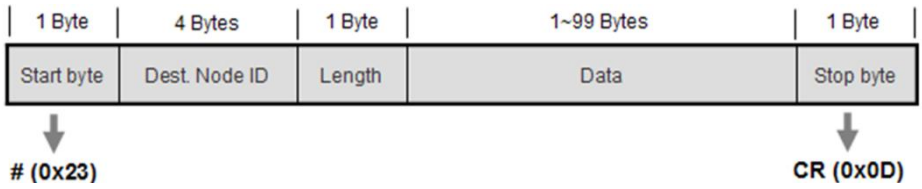
Channel

Default	11
Options	11 to 26
Description	The 2.4GHz channel. The range is from 11 to 26.

Output Power

Default	4.5
Options	Supports -20, -16, -12, -8, -4, -1.5, 1, 4.5 dBm
Description	The output from power side

Advanced Settings

Advanced Settings	Advanced Settings
Mode	Transparent or Addressable
Description	Transparent: All data comes to the Coordinator via the Ethernet port; the Coordinator will broadcast to the desired ZigBee node. Addressable: All data with specified frame format that comes to the Coordinator will be sent directly to the desired ZigBee node. The frame format should be represented as below:  Start byte: The head of the addressable mode command format, which can be modified by the option Start Byte. Dest. Node ID: This field contains 4 bytes that indicate what the desired ZigBee node is. Length: The length field is a byte count of the following Data field. Data: The data will be sent to the serial device connected to the desired ZigBee node. Stop byte: The tail of the addressable mode command format. This example shows how to send the data "ABCD" to the ZigBee node with ID 3. Start Byte: 0x23 | Dest. Node ID: 0x30 0x30 0x30 0x33 | Length: 0x04 | Data: 0x41 0x42 0x43 0x44 | Stop Byte: 0x0D

Start Byte

Default	# (0x23)
Options	0x00~0xFF
Description	The head of addressable mode command format on Coordinator.

Security Settings

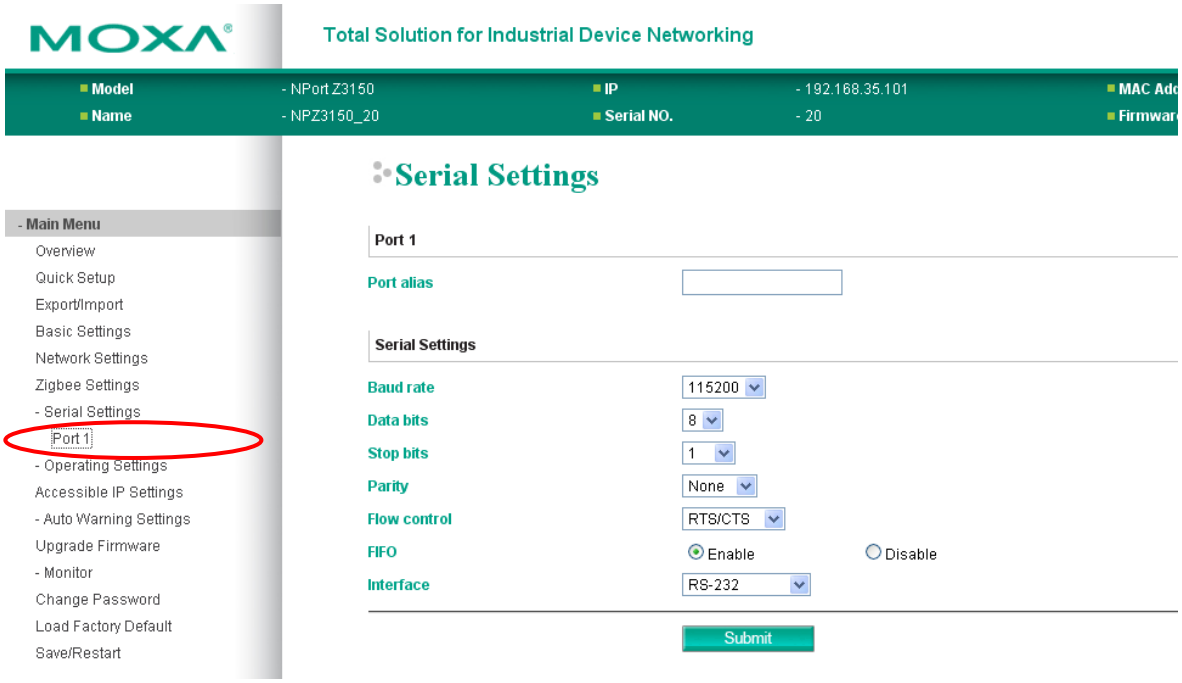
Encryption/Decryption

Default	Disable
Options	Enable or Disable
Description	AES encryption for Zigbee security

AES 128-bits Key

Default	
Options	HEX codes, from 0-9 and A-F
Description	Supply 128-bit AES data encryption. Use the following rule to input the AES key. Example: (BIN) 1101 1111 0010 1101 0001 … 0101 1011 1110 0011 1000 0100 (HEX) D F 2 D 1 … 5 B E 3 8 4 Input the following values into the key field: DF2D1…5BE384 (total of 16 bytes with 32 HEX code characters.)

Serial Settings > Port 1



The **Serial Settings** page for the serial port is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.

Port Alias

Default	
Options	free text (e.g., "Secondary console connection")
Description	This is an optional free text field to help you differentiate one serial port from another. It does not affect operation of the NPort device server.

ATTENTION

Serial communication settings should match the attached serial device. Check the communication settings in the user's manual for your serial device.

Baud Rate

Default	115200
Options	50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
Description	This field specifies the baudrate for the serial port. 50 to 921600: The serial port will operate at the specified baudrate

Data Bits

Default	8
Options	5, 6, 7, 8
Description	This field specifies the number of data bits used to encode each character of data.

Stop Bits

Default	1
Options	1, 1.5, 2
Description	This field specifies the number of stop bits used for each character frame.

Parity

Default	None
Options	None, Odd, Even, Space, Mark
Description	This field specifies the type of parity bit used for each character frame.

Flow Control

Default	RTS/CTS
Options	None, RTS/CTS, XON/XOFF, DTR/DSR
Description	This field specifies the type of flow control used by the serial port.

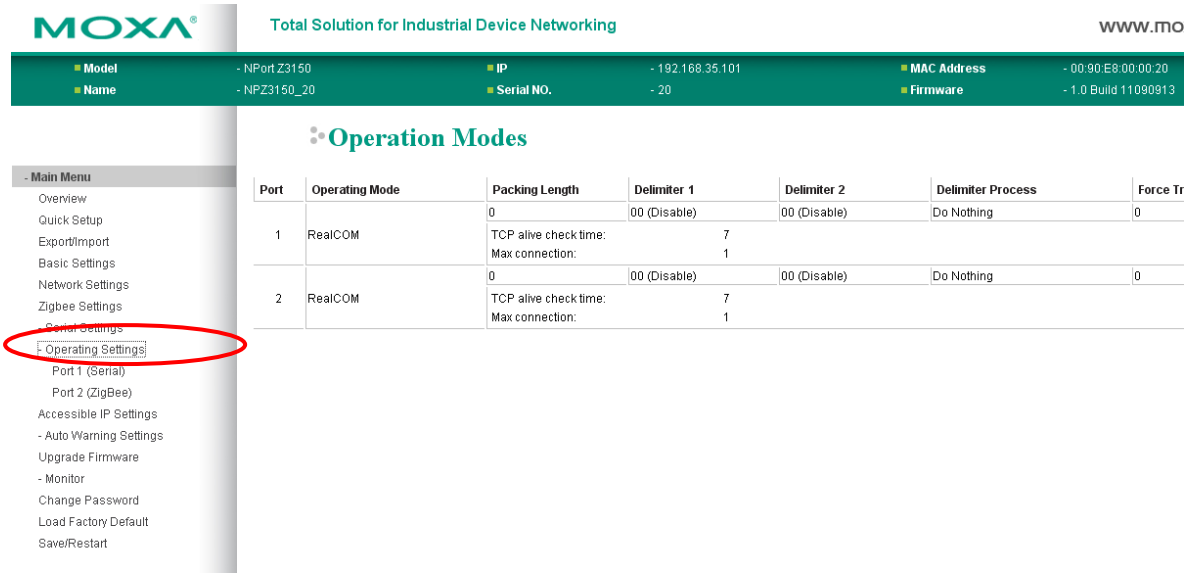
FIFO

Default	Enable
Options	Enable, Disable
Description	This field specifies whether the serial port will use the built-in FIFO. A 128-byte FIFO is provided to each serial port for both Tx and Rx directions. To prevent data loss during serial communication, this should be set to Disabled if the attached serial device does not have a FIFO.

Interface

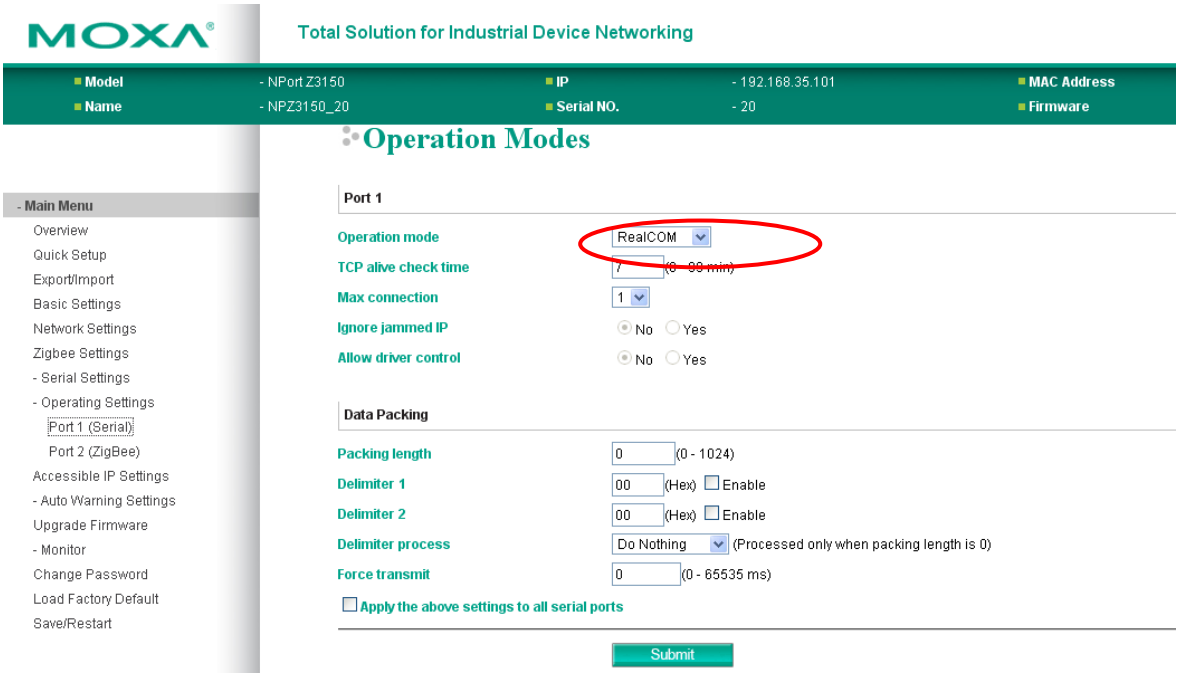
Default	RS-232
Options	RS-232, RS-422, RS-485 2-wire, RS-485 4-wire
Description	This field specifies the type of interface the serial port will use.

Operating Settings > Port 1 or 2



Click **Operating Settings**, located under **Main Menu**, to display the operating settings for both of NPort Z3150's serial ports. Port 1 is for serial port, beside, port 2 is for ZigBee port.

Settings for RealCOM Mode



When **Mode** is set to RealCOM on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Max connection**, and **Ignore jammed IP**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Max Connection

Default	1
Options	1 to 8
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only one specific host can access this serial port, and the Real COM driver on that host will have full control over the port. 2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the Real COM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the NPort rather than by your application program. Application software that is based on the Real COM driver will receive a driver response of "success" when using any of the Win32 API functions. The NPort will send data only to the Real COM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.

ATTENTION

When Max connection is 2 or greater, the serial port's communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the NPort. Any host that opens the COM port connection must use identical serial communication settings.

Ignore Jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Allow Driver Control

Default	Disable
Options	Disable, Enable
Description	This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. Disable: Driver control commands will be ignored. Enable: Control commands will be accepted, with the most recent command received taking precedence.

Connection Goes Down

Default	always high
Options	always low, always high
Description	This field specifies what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Always low: The selected signal will change to low when the Ethernet connection goes down. Always high The selected signal will remain high when the Ethernet connection goes down.

Packet Length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 0x00 to 0xFF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

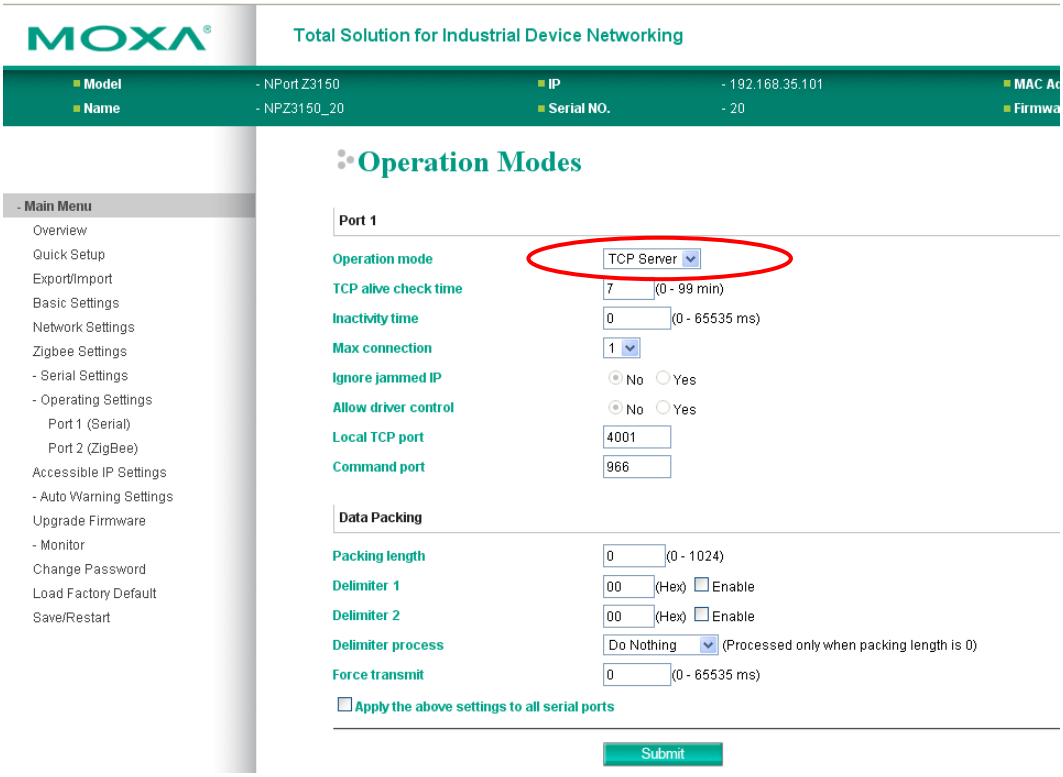
Delimiter Process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Server Mode



When **Mode** is set to **TCP Server** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Max connection**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Inactivity Time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.

Max Connection

Default	1
Options	1 to 8
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only a single host may open the TCP connection to the serial port. 2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. When multiple connections are established, serial data will be duplicated and sent to all connected hosts. Data from hosts will be sent to the attached serial device on a first-in-first-out basis.

Ignore Jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Allow Driver Control

Default	Disable
Options	Disable, Enable
Description	This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. Disable: Driver control commands will be ignored. Enable: Control commands will be accepted, with the most recent command received taking precedence.

TCP Port

Default	4001
Options	0 to 9999
Description	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

Command Port

Default	966
Options	0 to 9999
Description	This field specifies the TCP port number for listening to SSDK commands from the host.

Packet Length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 0x00 to 0xFF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

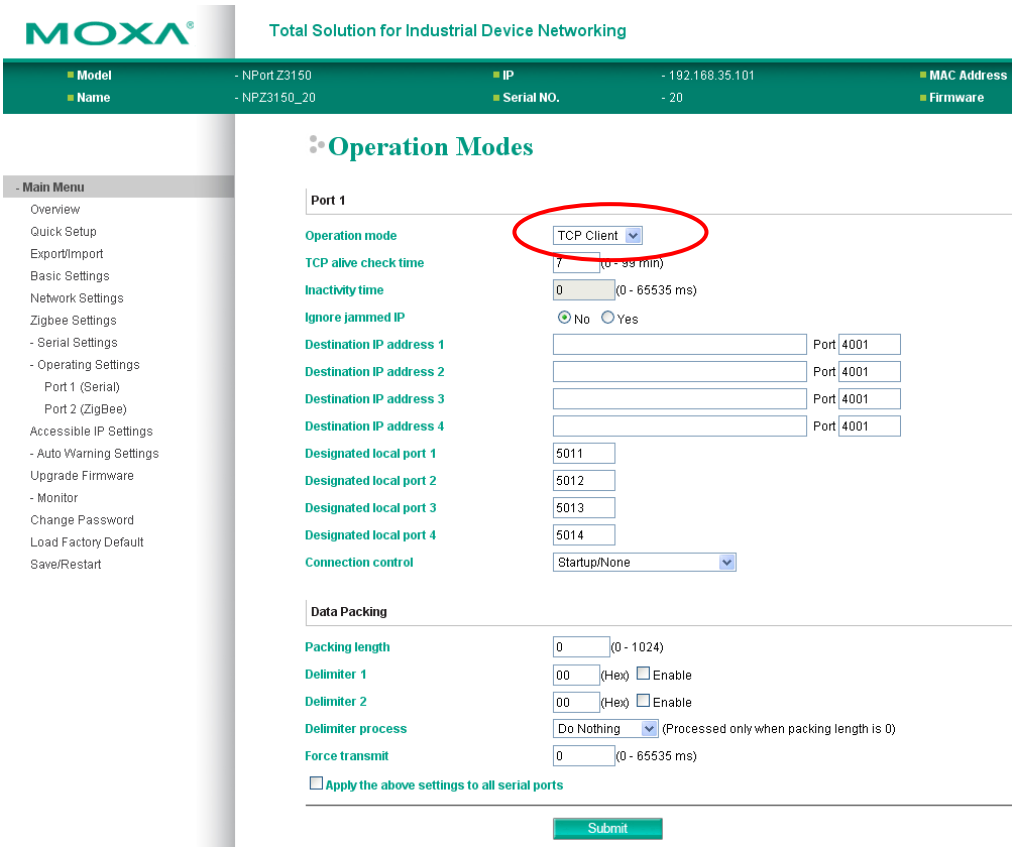
Delimiter Process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Client Mode



When **Mode** is set to **TCP Client** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Ignore jammed IP**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Inactivity Time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The TCP connection will be kept active until a connection close request is received, even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted. **Connection Control** must be set to "Any character/Inactivity time" for this setting to have effect.

Ignore Jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Destination Address 1 to 4

Default	
Options	IP address and port (e.g., "192.168.1.1" and "4001")
Description	This field specifies the remote host(s) that will access the attached device. At least one destination must be provided. This field supports the use of domain names and names defined in the host table.

ATTENTION

In TCP Client mode, up to 4 connections can be established between the serial port and TCP hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

Designated Local Port 1 to 4

Default	
Options	1 to 65535
Description	This field specifies the TCP port number that will be used for data transmission with the serial port.

Connection Control

Default	Startup/None
Options	Startup/None, Any Character/None, Any Character/Inactivity Time, DSR On/DSR Off, DSR On/None, DCD On/DCD Off, DCD On/None
Description	This field specifies how connections to the device are established and closed. Startup/None: The connection will be opened as the NPort starts up. The connection will only be closed manually. Any Character/None: The connection will be opened as soon as a character is received from the attached device. The connection will only be closed manually. Any Character/Inactivity Time: The connection will be opened as soon as a character is received from the attached device. The connection will be closed if no data is received for the time specified in Inactivity time. DSR On/DSR Off: The TCP connection is opened when the DSR signal is on, and closed when the DSR signal is off. DSR On/None: The TCP connection is opened when the DSR signal is on. The connection will only be closed manually. DCD On/DCD Off: The TCP connection is opened when the DCD signal is on, and closed when the DCD signal is off. DCD On/None: The TCP connection is opened when the DCD signal is on. The connection will only be closed manually.

Packet Length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 0x00 to 0xFF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

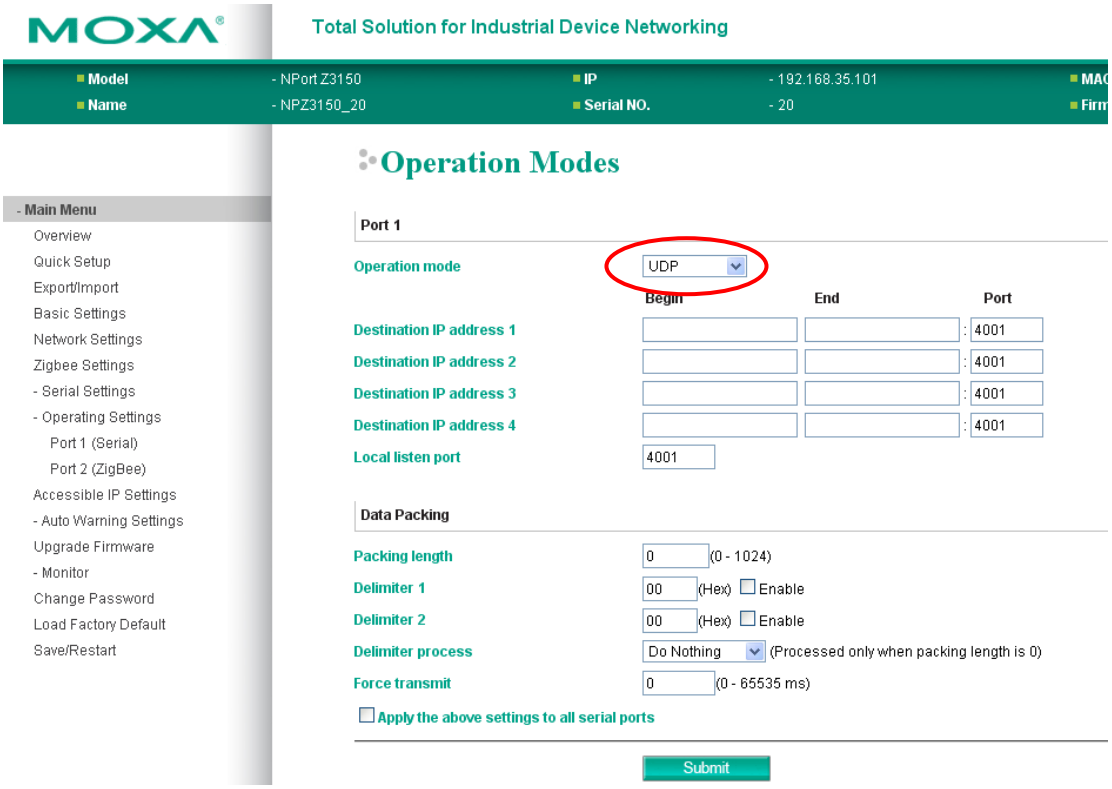
Delimiter Process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for UDP Mode



When **Mode** is set to **UDP** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **Destination address 1** through **4**, **Local listen port**, and **Packet length**.

Destination Address 1 to 4

Default	
Options	IP address range and port (e.g., "192.168.1.1" to "192.168.1.64" and "4001")
Description	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided. The maximum selectable IP address range is 64 addresses. However, you can enter multicast addresses in the Begin field, in the form xxx.xxx.xxx.255. For example, enter "192.127.168.255" to allow the NPort to broadcast UDP packets to all hosts with IP addresses between 192.127.168.1 and 192.127.168.254.

Local Listen Port

Default	4001
Options	0 to 9999
Description	This field specifies the UDP port that the NPort listens to and that other devices must use to contact the attached serial device.

Packet Length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 0x00 to 0xFF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

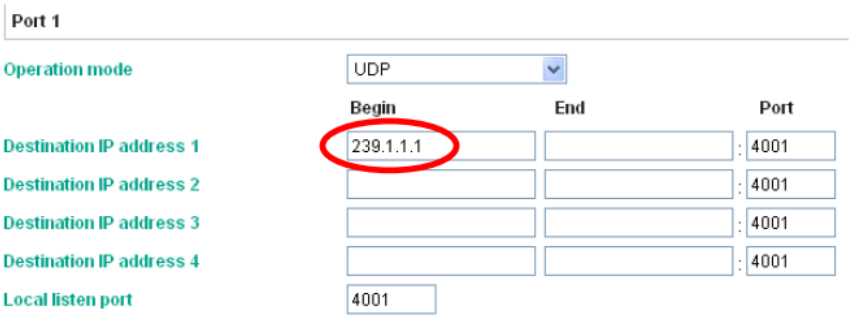
Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

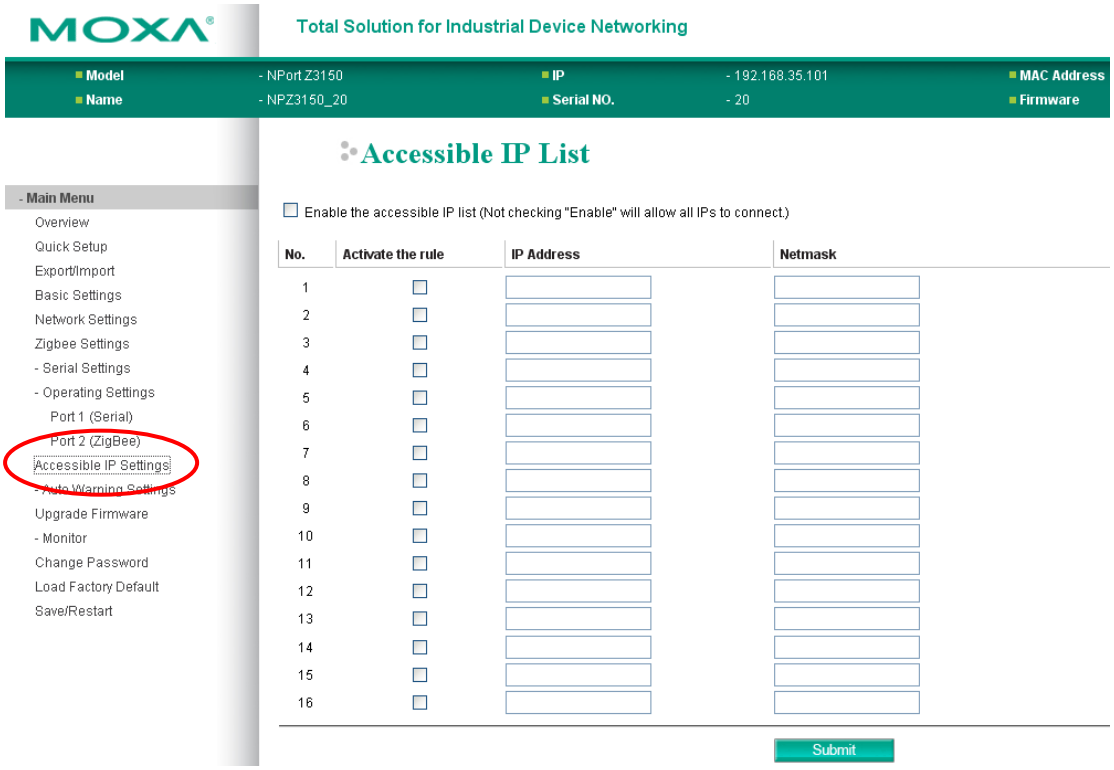
UDP Multicast

A multicast is a packet sent by one host to multiple hosts. In multicast, each host that belongs to a specific multicast group will receive multicast packets for that group. To configure a host as a multicast receiver over the Internet, it must inform the routers on its LAN. The Internet Group Management Protocol (IGMP) is used to communicate group membership information between hosts and routers on a LAN. The NPort Z3150 supports IGMP version 2.



You could key in the IP (ex. 239.1.1.1) that multicast group assigned into the column of Destination IP address, and next, NPort would automatically add the Group, receiving all packets from this group in order to fulfill the function of multicast.

Accessible IP Settings



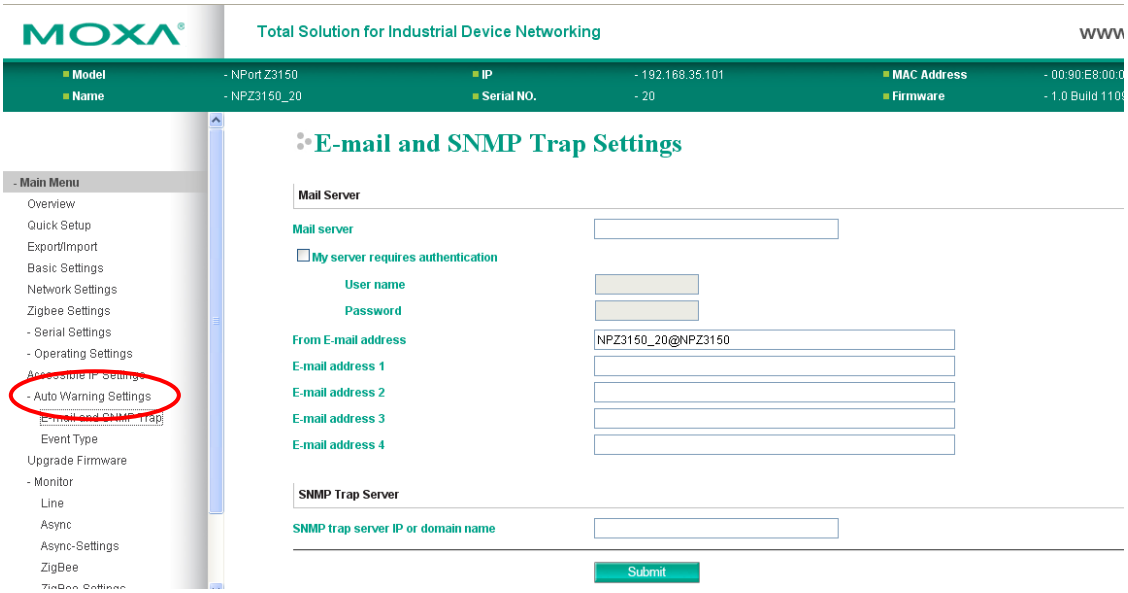
The NPort Z3150 uses an IP address based filtering method to control access to itself.

Accessible IP Settings allows you to add or block remote host IP addresses to prevent unauthorized access. Access to NPort Z3150 is controlled by IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed to access the NPort Z3150. You can allow one of the following cases by setting the parameter.

- **Only one host with a specific IP address can access the NPort Z3150**
  Enter "IP address/255.255.255.255" (e.g., "192.168.1.1/255.255.255.255").
- **Hosts on a specific subnet can access the NPort Z3150**
  Enter "IP address/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0").
- **Any host can access the NPort Z3150**
  Disable this function by un-checking the "Enable the accessible IP list" checkbox. Refer to the following table for more configuration examples.

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Auto Warning Settings > E-mail and SNMP Trap > E-mail server



The **E-mail Alert** page is located under **E-mail and SNMP Trap** in the **Auto Warning Settings** folder. This is where you specify how and where e-mail is sent when e-mail is used for automatic notification of system and serial port events.

ATTENTION

Consult your network administrator or ISP for the mail server settings to use for your network. If these settings are not configured correctly, e-mail notification may not work properly.

Mail Server

Default	
Options	free text (e.g., "192.168.3.3")
Description	This field specifies the IP address of the mail server that will be used when sending automatic warning e-mails. If the mail server requires authentication, select "My server requires authentication" and enter the username and password.

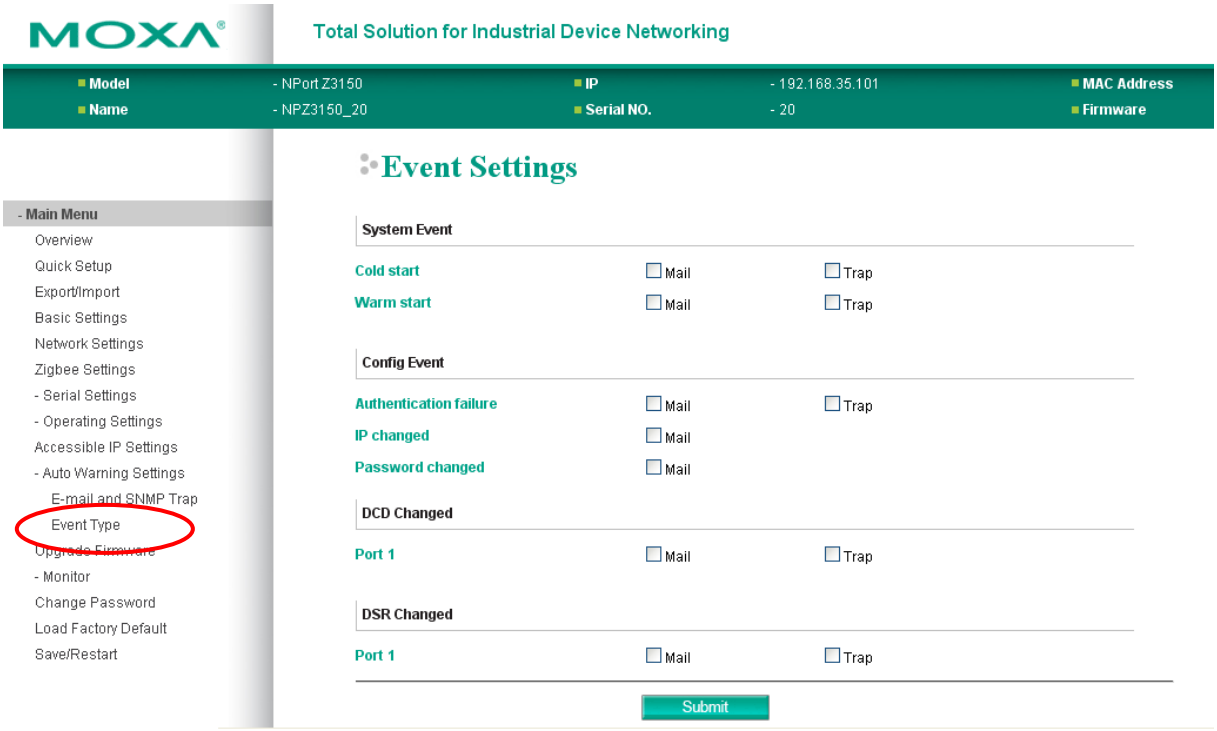
From E-mail Address

Default	
Options	free text (e.g., "jsmith@xyz.com")
Description	This field specifies the e-mail address that will be listed in the e-mail's "From" field.

SNMP Trap Server IP

Default	
Options	IP address (e.g., "192.168.5.5")
Description	This field specifies the IP address of the SNMP trap server that will receive SNMP traps.

Auto Warning Settings > Event Settings



The **Event Settings** page is located under **Event Settings** in the **Auto Warning Settings** folder. This is where you specify how the NPort will notify you of system and configuration events. Depending on the event, different options for notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

Event	Description
Cold start	The NPort was powered on, or was restarted after a firmware upgrade.
Warm start	The NPort restarted without powering off.
Authentication failure	An attempt has been made to open the web, Telnet, or serial console, but the password was incorrect.
IP changed	The IP address has been changed.
Password changed	The password to the console has been changed.

DCD changed

The DCD (Data Carrier Detect) signal has changed, also indicating that the modem connection status has changed. For example, a DCD change to high also means "Connected" between local modem and remote modem. If the DCD signal changes to low, it also means that the connection line is down.

When the DCD changes, the NPort Z3150 will immediately send an e-mail or send an SNMP trap.

DSR changed

The DSR (Data Set Ready) signal has changed, also indicating that the data communication equipment's power is off. For example, a DSR change to high also means that the DCE is powered ON. If the DSR signal changes to low, it also means that the DCE is powered off.

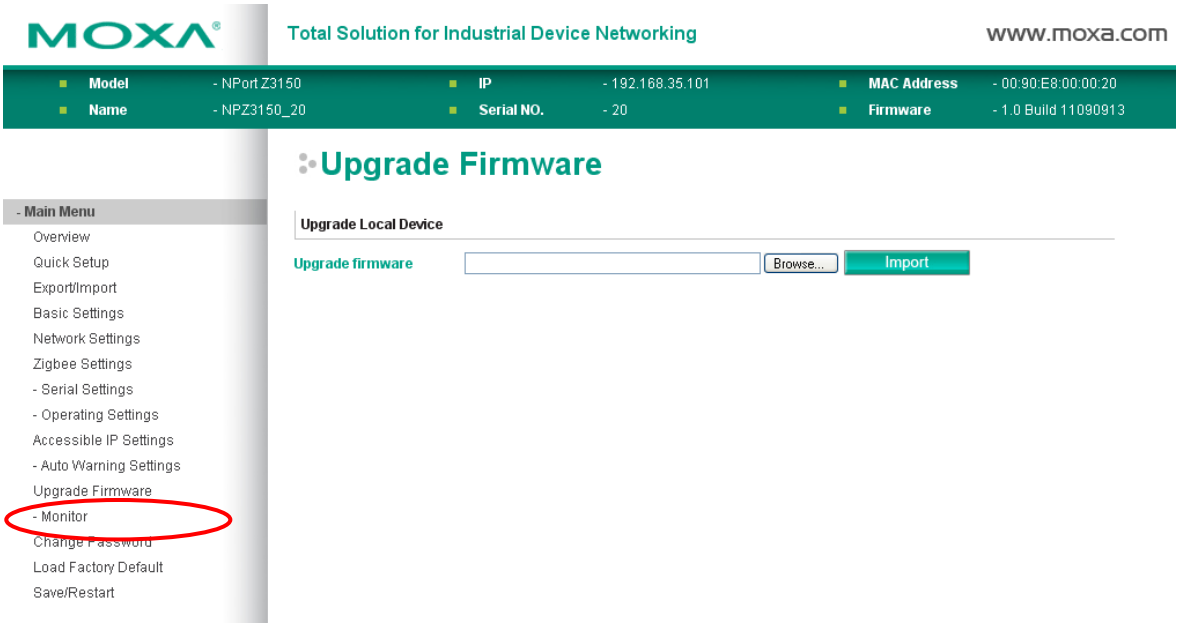
When the DSR changes, the NPort Z3150 will immediately send an e-mail or send an SNMP trap.

Event	Description
Mail	This feature helps the administrator manage how the NPort Z3150 sends e-mail to pre-defined e-mail boxes when the enabled events—such as Cold start, Warm start, Authentication failure, etc.—occur. To configure this feature, click the Event Type Mail checkbox.
Trap	This feature helps the administrator manage how the NPort Z3150 sends SNMP Trap to a pre-defined SNMP Trap server when the enabled events—such as Cold start, Warm start, Authentication failure, etc.—occur. To configure this feature, click the Event Type Trap checkbox.

ATTENTION

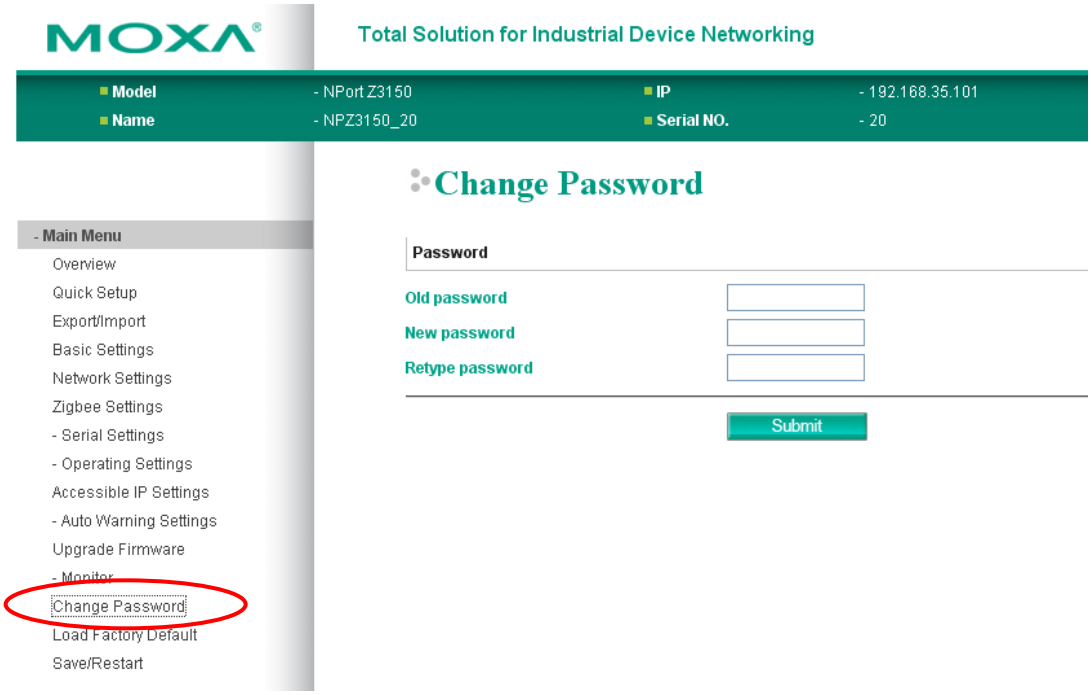
SNMP indicates a change in DCD or DSR signals but does not differentiate between the two. A change in either signal from "–" to "+" is indicated by "link up" and a change in either signal from "+" to "–" is indicated by "link down."

Firmware Upgrade



The **Firmware Upgrade** page is where you can update the NPort firmware. After obtaining the latest firmware from www.moxa.com, select or browse for the firmware file in the **Select firmware file** field. Before clicking **[Import]**, it is a good idea to save the NPort configuration using the **Import/Export** page, since the firmware upgrade process may cause all settings to revert to factory defaults.

Change Password



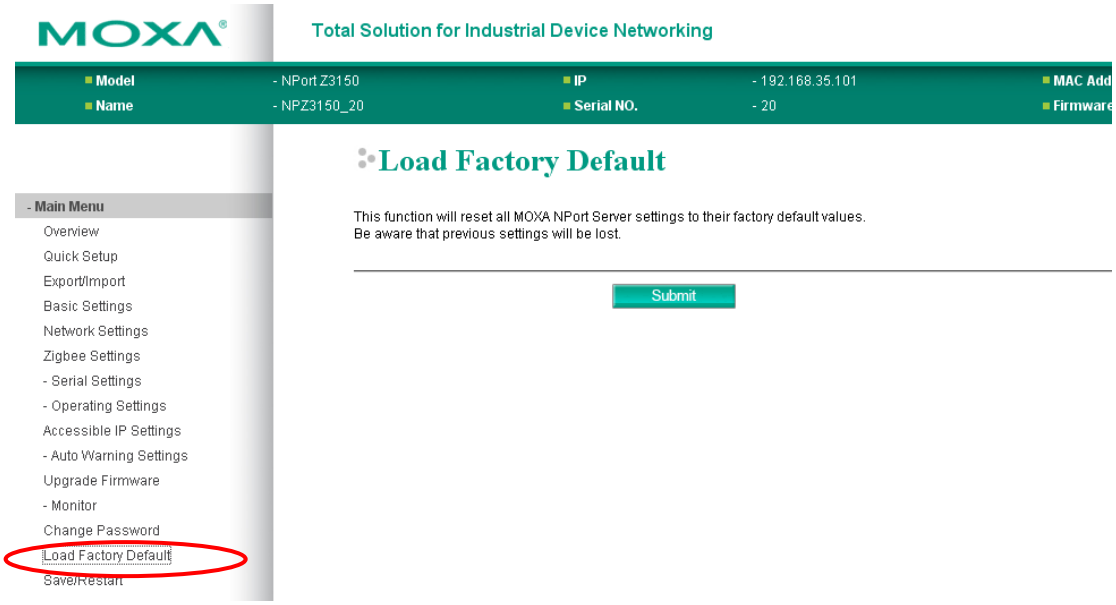
The **Change Password** page is used to change the password, first enter the old password in the **Old password** field. Leave this blank if the NPort is not currently password-protected. Enter the new password twice, once in the **New password** field and once in the **Retype password**. Leave these fields blank to remove password protection.

ATTENTION

If you forget the password, the ONLY way to configure the NPort is by loading the factory defaults with the reset button. All settings will be lost.

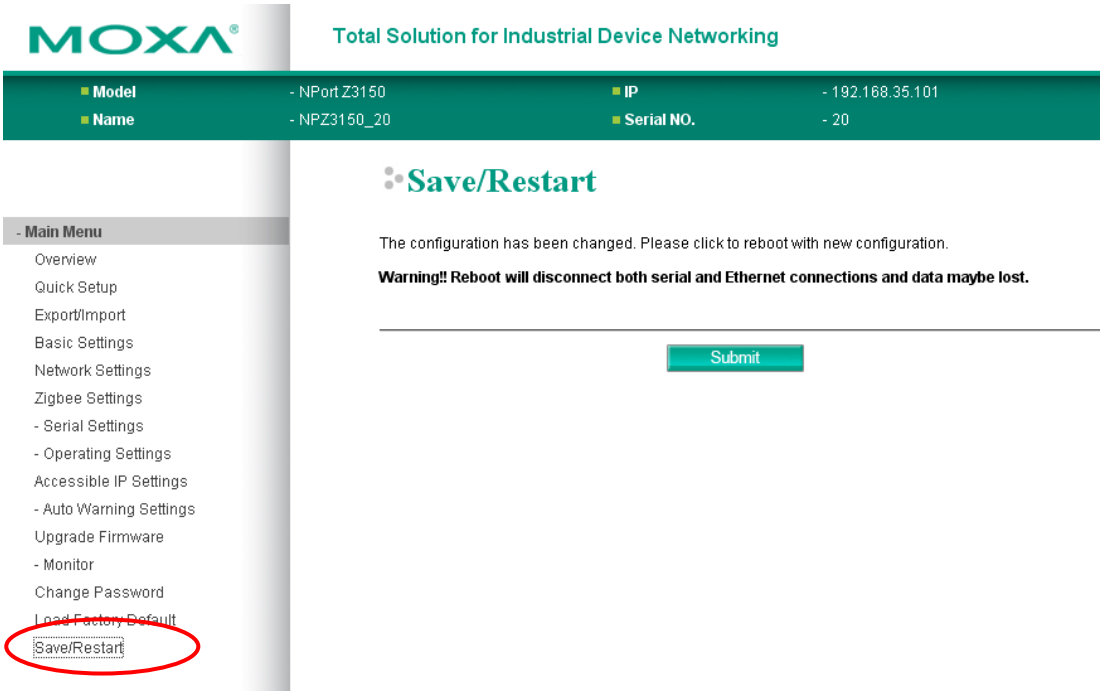
Before setting the password, you may want to first export the configuration to a file. Your configuration can then be easily imported back into the NPort if necessary.

Load Factory Default



The **Load Factory Default** page is used to recovery default settings. Click **[Submit]** to reset all settings to the factory defaults.

Save/Restart



The **Save/Restart** page is used to save configuration settings and then reboot device. Click **[Submit]** to save configuration settings into device and then restart the NPort. All new settings will be applied after device restarts.

6

Web Console: Monitor

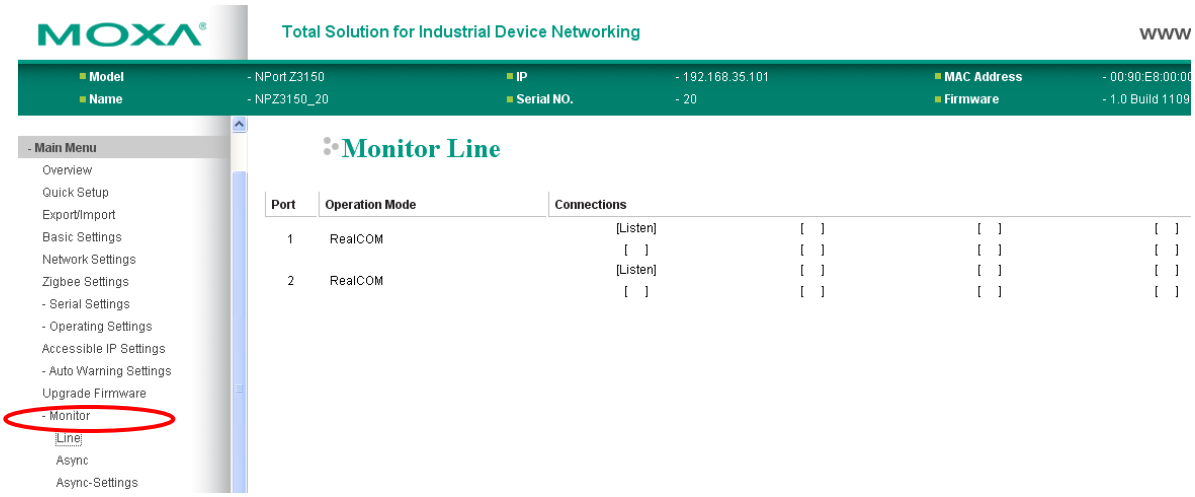
The following topics are covered in this chapter:

- **Overview**
- **Monitor Line**
- **Monitor Async**
- **Monitor Async-Settings**
- **Monitor ZigBee**
- **Monitor ZigBee-Settings**

Overview

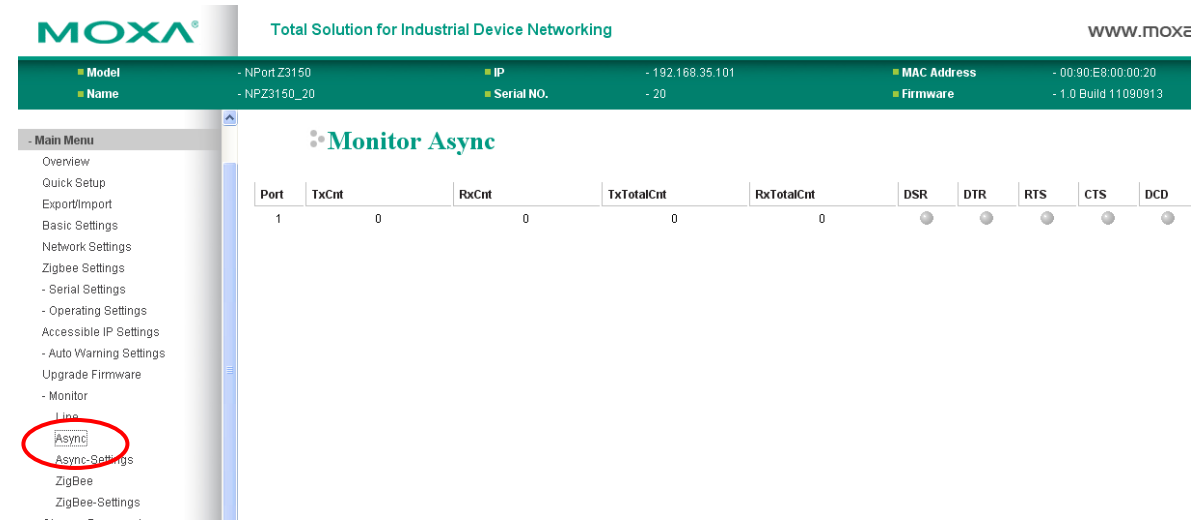
This chapter explains how to use the **Monitor** functions on the NPort web console. These functions allow you to monitor many different aspects of operation.

Monitor Line



The **Monitor Line** page is used to monitor the current operation mode and host connection status for each port.

Monitor Async



The **Monitor Async** is used to monitor the signal and data transmission status for the serial port.

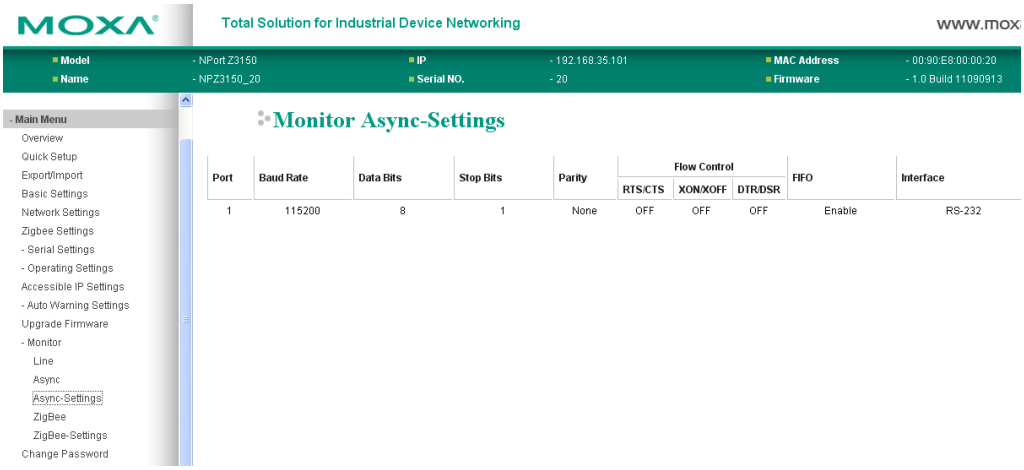
TxCnt: number of Tx packets (to device) for the current connection

RxCnt: number of Rx packets (from device) for the current connection

TxTotalCnt: number of Tx packets since the NPort was powered on

RxTotalCnt: number of Rx packets since the NPort was powered on

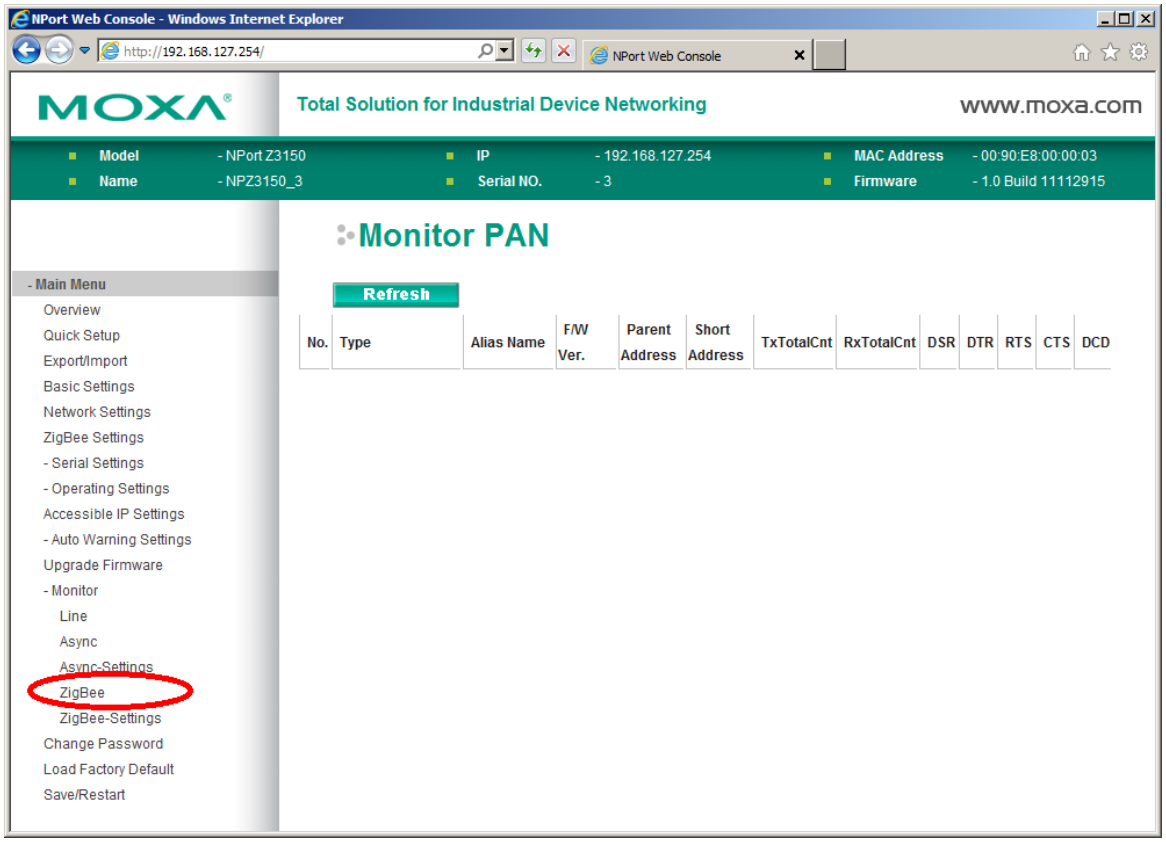
Monitor Async-Settings



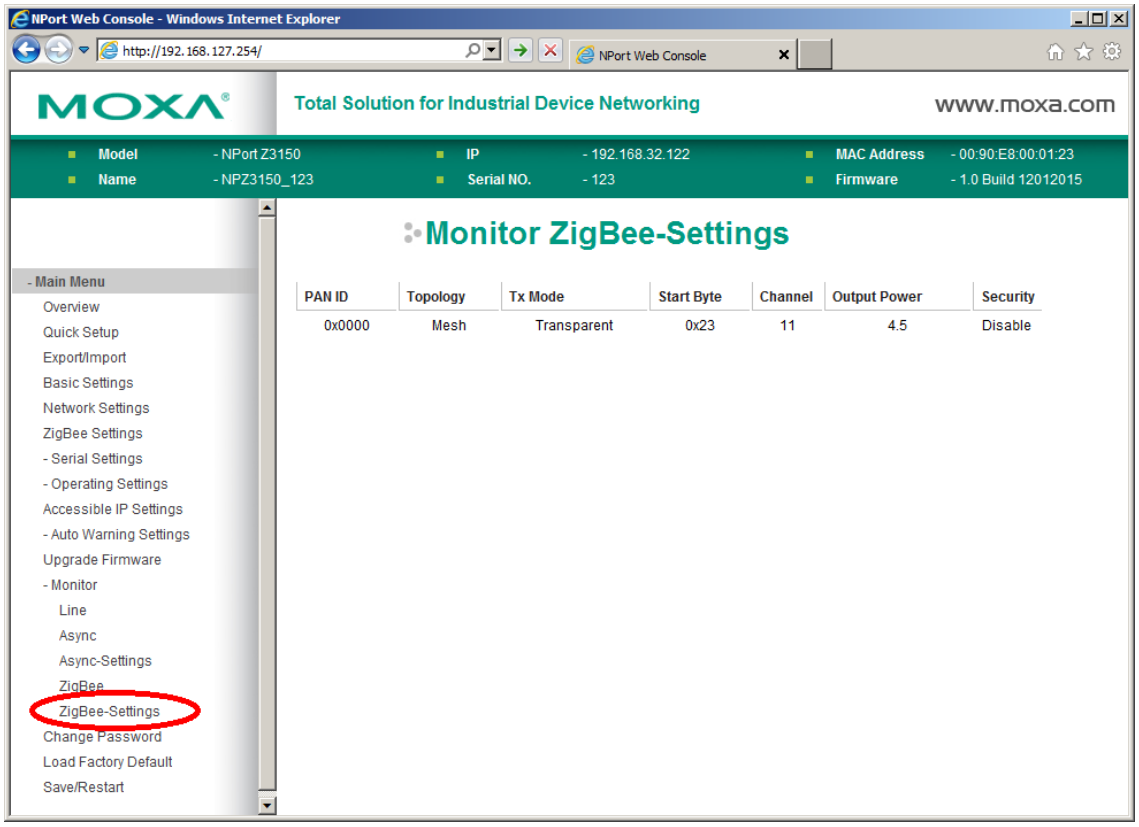
The **Monitor Async-Settings** page is used to view the current communication settings for the serial port.

Monitor ZigBee

The **ZigBee** page is used to view the current status of ZigBee network connection.



Monitor ZigBee-Settings



The **ZigBee-Settings** page is used to view the current status of the NPort Z3150 itself.

7

Installing and Configuring the Software

The following topics are covered in this chapter:

- **Overview**
- **NPort Windows Driver Manager**
  - Installing NPort Windows Driver Manager
  - Adding Mapped Serial Ports
  - Configuring Mapped Serial Ports
- **NPort Search Utility**
  - Installing NPort Search Utility
  - Finding NPort Device Servers on Network
  - Modifying NPort IP Addresses
  - Upgrading NPort Firmware
- **Linux Real TTY Drivers**
  - Basic Steps
  - Installing Linux Real TTY Driver Files
  - Mapping TTY Ports
  - Removing Mapped TTY Ports
  - Removing Linux Driver Files
- **UNIX Fixed TTY Drivers**
  - Installing the UNIX Driver
  - Configuring the UNIX Driver

Overview

This chapter describes how to install and use NPort Windows Driver Manager, NPort Search Utility, and NPort Linux and UNIX drivers. These items are located on the Document & Software CD that is provided with the NPort Z3150.

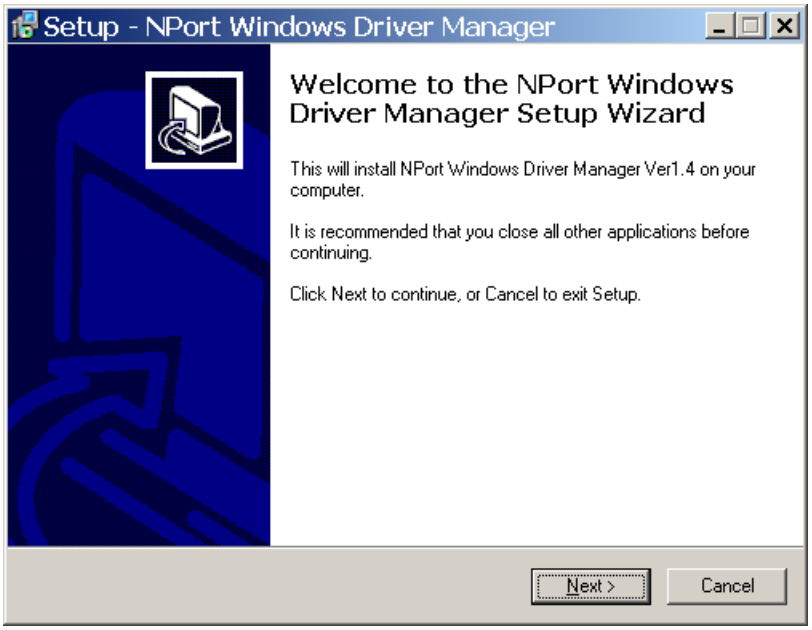
NPort Windows Driver Manager is a utility that installs and manages NPort COM drivers for COM mapping. **NPort Search Utility** is a utility for the management of NPort device servers over the network. You may also use NPort Search Utility to upgrade the firmware.

NPort Windows Driver Manager

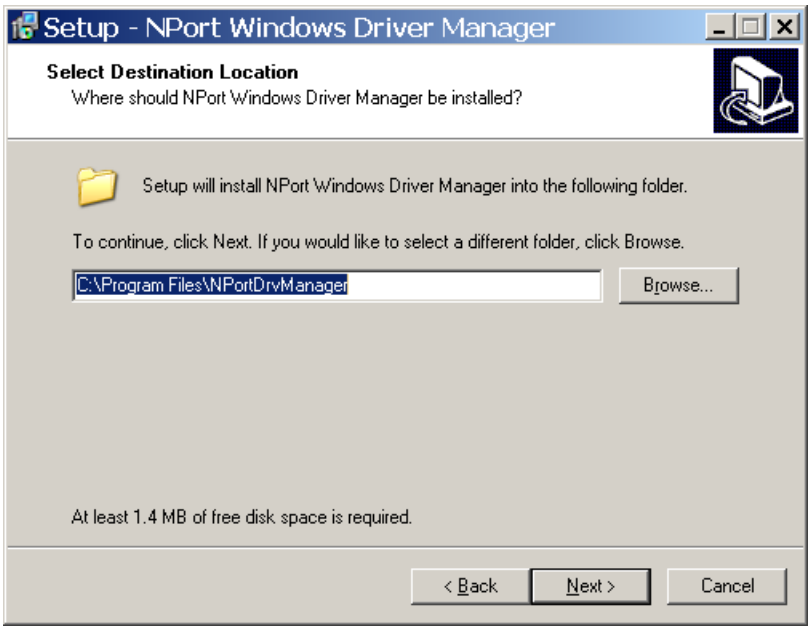
NPort Windows Driver Manager installs remote NPort serial ports as new COM ports on your Windows PC. When the drivers are installed and configured, devices that are attached to serial ports on the NPort will be treated as if they were attached to your PC's own COM ports. The NPort serial port must be configured for Real COM mode when being mapped to a COM port.

Installing NPort Windows Driver Manager

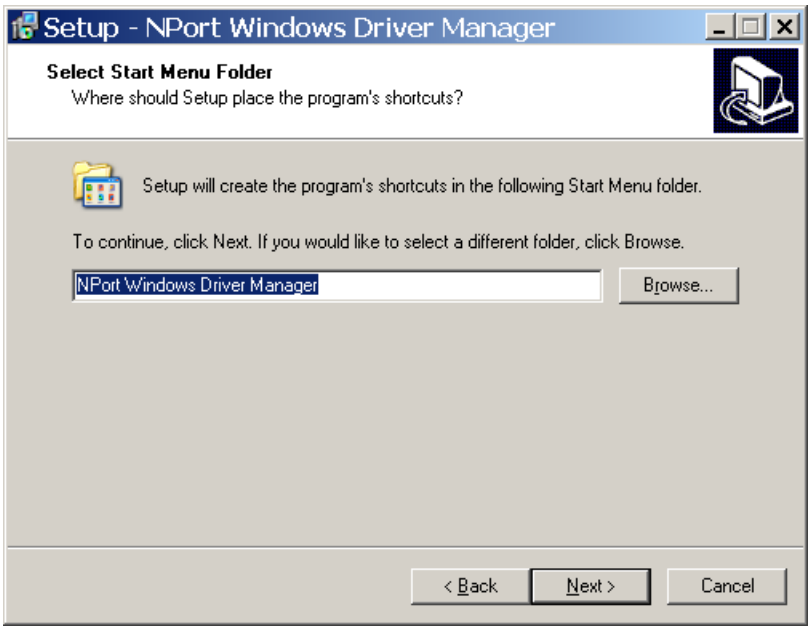
1. The main installation window will open when you insert the Document & Software CD. Click **[INSTALL COM Driver]** to proceed. Once the installation program starts running, click **[Yes]** to proceed.
2. The installation wizard will open. Click **[Next]** to proceed.


Setup - NPort Windows Driver Manager
Welcome to the NPort Windows Driver Manager Setup Wizard
This will install NPort Windows Driver Manager Ver1.4 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

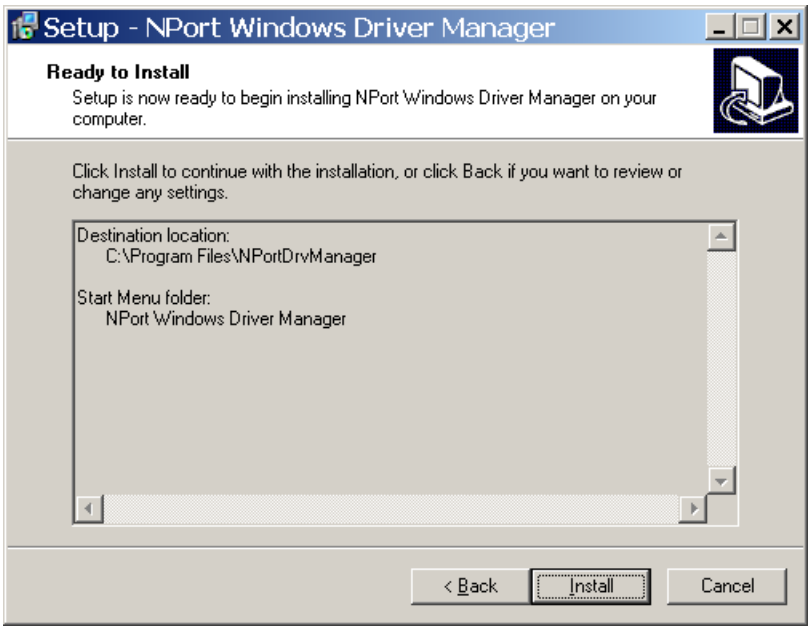
3. Select a destination directory and click **[Next]** to proceed.


Setup - NPort Windows Driver Manager
Select Destination Location
Where should NPort Windows Driver Manager be installed?
Setup will install NPort Windows Driver Manager into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\NPortDrvManager
Browse...
At least 1.4 MB of free disk space is required.
< Back
Next >
Cancel

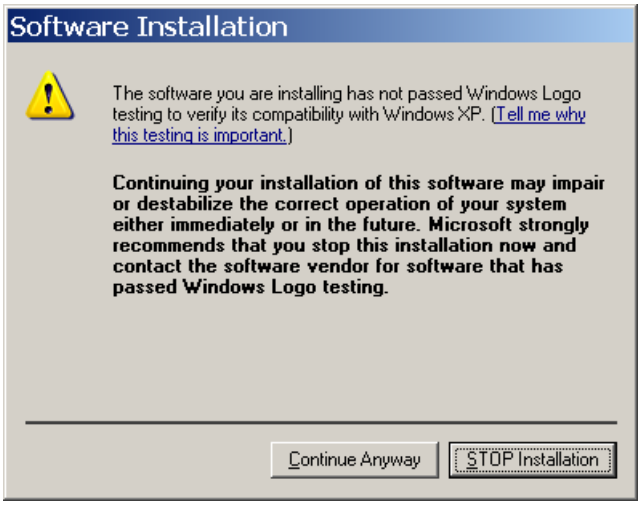
4. Select a folder for the program shortcuts and click **[Next]** to proceed.


Setup - NPort Windows Driver Manager
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
NPort Windows Driver Manager
Browse...
< Back
Next >
Cancel

5. Verify the installation parameters and click **Install** to proceed.


Setup - NPort Windows Driver Manager
Ready to Install
Setup is now ready to begin installing NPort Windows Driver Manager on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\NPortDrvManager
Start Menu folder:
NPort Windows Driver Manager
< Back
Install
Cancel

6. If you see a warning that the software has not passed Windows Logo testing, click **[Continue Anyway]** to proceed.


Software Installation
The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the software vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

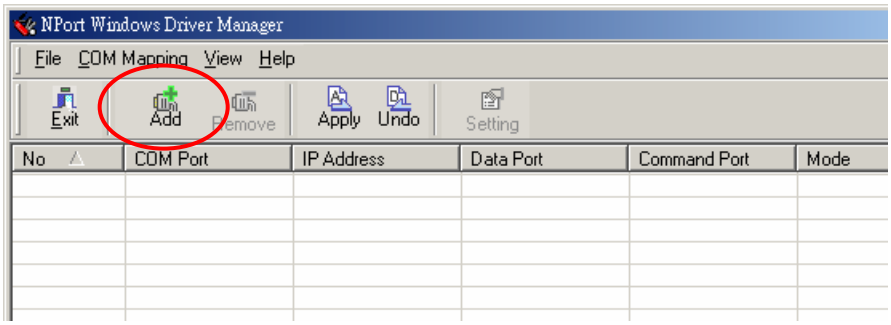
7. The wizard will begin installing the files. When the files have been installed, click **[Finish]** to complete the installation.

Setup - NPort Windows Driver Manager
Completing the NPort Windows Driver Manager Setup Wizard
Setup has finished installing NPort Windows Driver Manager on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch NPort Windows Driver Manager
Finish

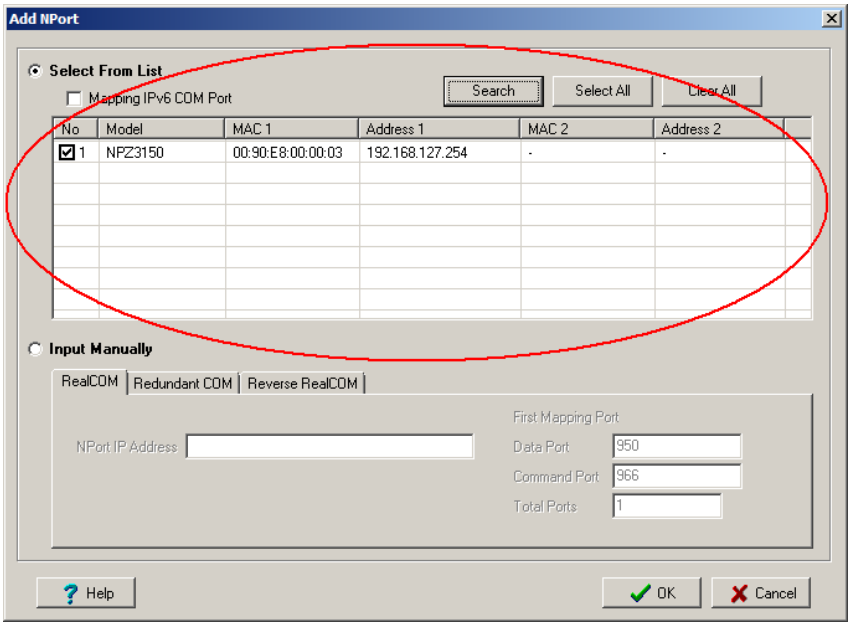
Adding Mapped Serial Ports

NPort Windows Driver Manager adds a COM port to your PC that is mapped to an NPort serial port. The destination NPort serial port must be set to Real COM mode.

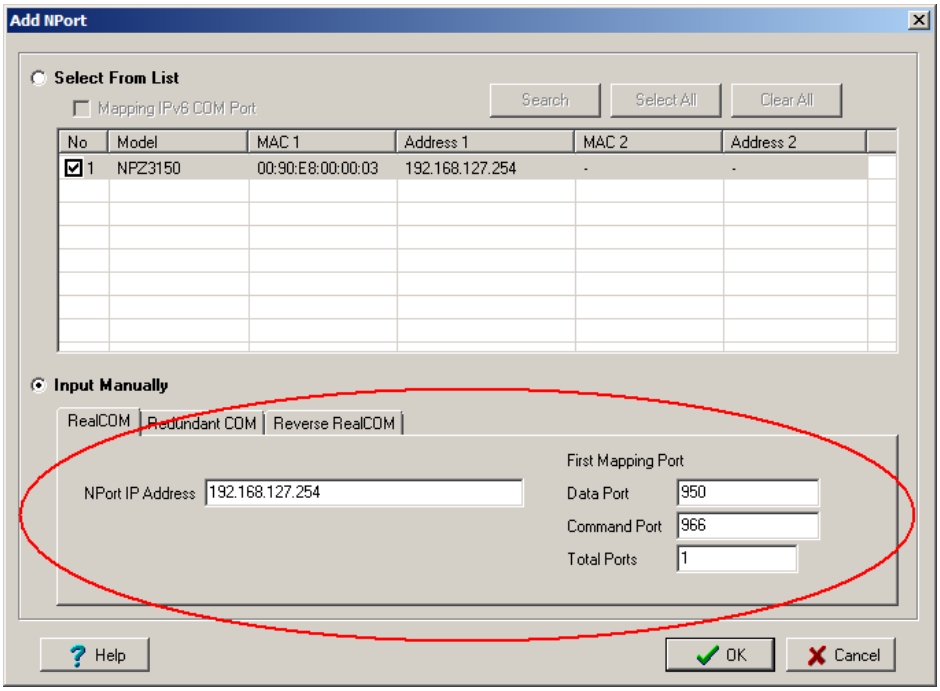
1. In **NPort Windows Driver Manager**, click **[Add]** on the main toolbar.



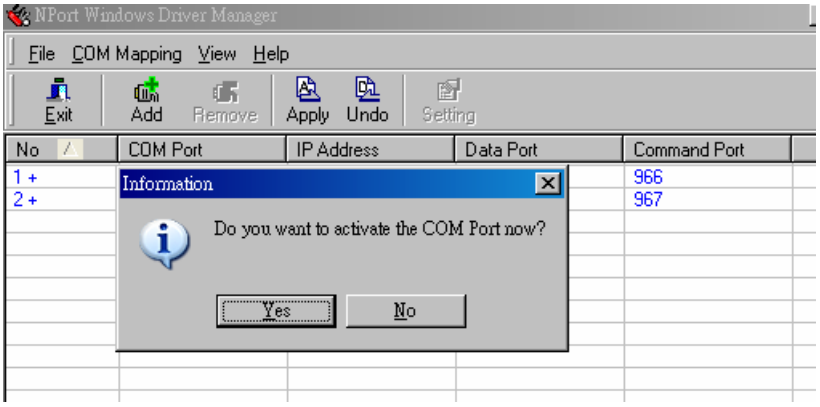
2. Click **[Search]** to search the network for NPort device servers. In the list of NPort device servers that are found, select the unit(s) that you will use for COM mapping and click **[OK]**.



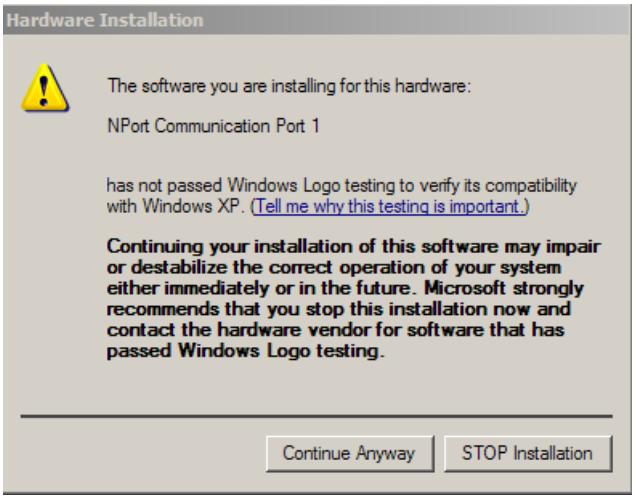
Alternatively, you can select **Input Manually** and manually enter the **NPort IP Address**, **1st Data Port**, **1st Command Port**, and **Total Ports** for the desired NPort unit. Click **[OK]** to proceed.



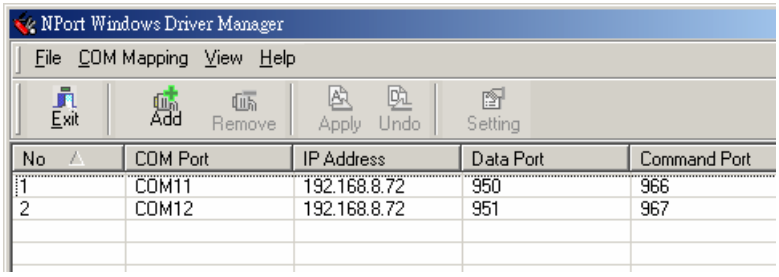
3. NPort Windows Driver Manager will list each available serial port and will automatically assign a new COM port to each one. The new COM port will not be accessible by the host system until it has been activated in NPort Windows Driver Manager. Activating a mapped COM port saves the information in the host system registry and makes the COM port available for use. Click **[Yes]** to activate the COM port(s) at this time; click **[No]** to activate the COM port(s) later.


NPort Windows Driver Manager
File COM Mapping View Help
Exit Add Remove Apply Undo Setting
No COM Port IP Address Data Port Command Port
1 + 966
2 + 967
Information
Do you want to activate the COM Port now?
Yes
No

4. For each mapped COM port that is activated, you may see a message indicating that the software has not passed Windows Logo certification. Click **[Continue Anyway]** to proceed.

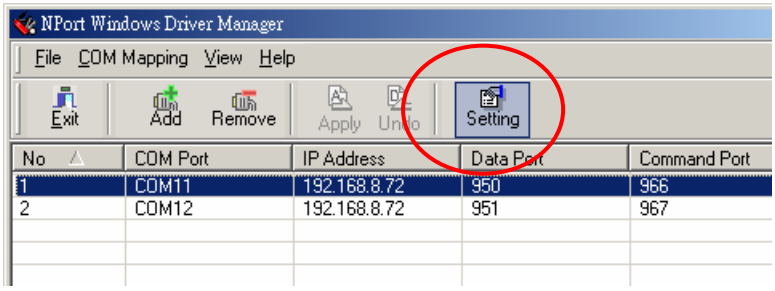

Hardware Installation
The software you are installing for this hardware:
NPort Communication Port 1
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

5. Activated COM ports will be listed in black; COM ports that have not been activated will be listed in blue. Once a COM port has been activated, the host computer will be able to communicate with the new COM port as if it were physically attached. Since the COM mappings are stored in the host system registry, they will still be in effect if the PC is restarted or if NPort Windows Driver Manager is closed.

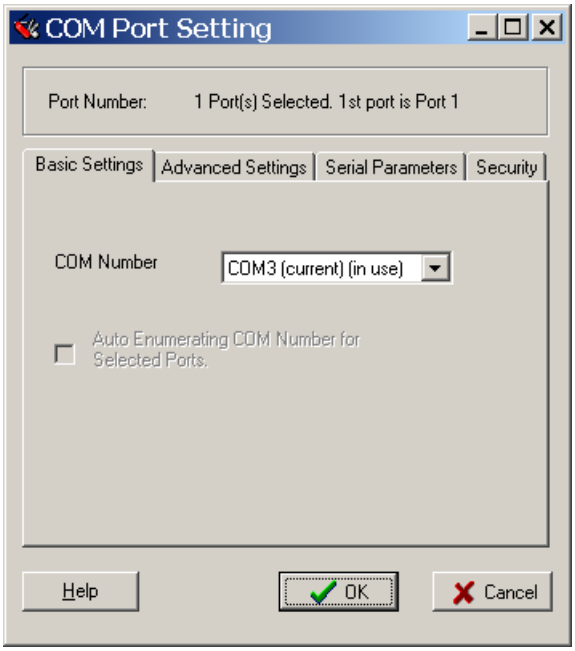

NPort Windows Driver Manager
File COM Mapping View Help
Exit Add Remove Apply Undo Setting
No COM Port IP Address Data Port Command Port
1 COM11 192.168.8.72 950 966
2 COM12 192.168.8.72 951 967

Configuring Mapped Serial Ports

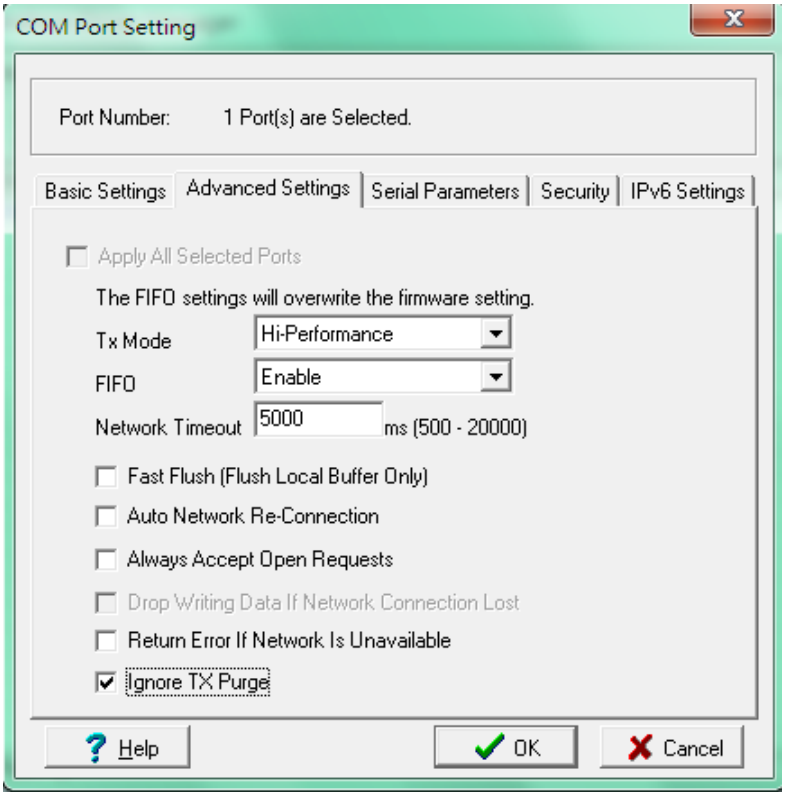
1. To modify the settings of a mapped serial port, select the desired port(s) and click **[Setting]** on the main toolbar.



2. On the **Basic Setting** tab, select the **COM Number** that will be assigned to the serial port. If you have selected multiple ports, you can assign COM numbers automatically in sequential order by selecting the "Auto Enumerating" function.



3. On the **Advanced Setting** tab, configure **Tx Mode**, **FIFO**, and **Fast Flush**.



Tx Mode: In Hi-Performance mode, the driver immediately issues a "Tx Empty" response to the program after sending data to the NPort. In Classical mode, the driver sends the "Tx Empty" response after confirmation is received from the NPort. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

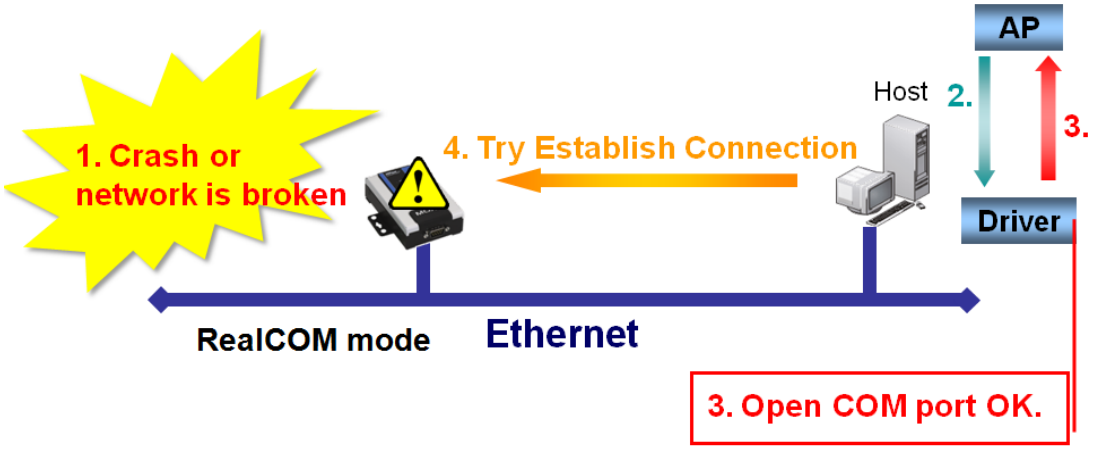
FIFO: This tells the driver whether or not to use the FIFO.

Network Timeout: You can use this option to prevent blocking if the target NPort is unavailable.

Auto Network Re-Connection: With this option enabled, the driver will repeatedly attempt to re-establish the TCP connection if the NPort does not respond to background "check alive" packets

Always Accept Open Requests

When the driver cannot establish a connection with the NPort, the user's software can still open the mapped COM port, just like an onboard COM port.



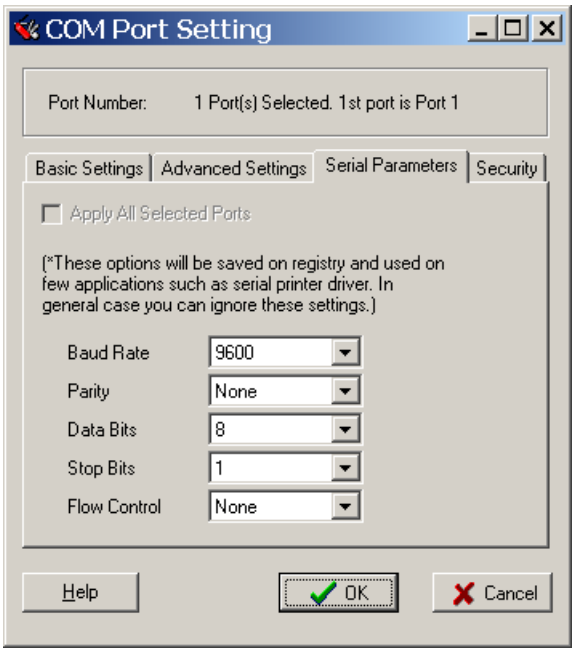
Return error if network is unavailable: If this option is disabled, the driver will not return any error even when a connection cannot be established to the NPort. With this option enabled, calling the Win32 Comm function will result in the error return code "STATUS_NETWORK_UNREACHABLE" when a connection cannot be established to the NPort. This usually means that your host's network connection is down, perhaps due to a cable being disconnected. However, if you can reach other network devices, it may be that the NPort is not powered on or is disconnected. Not that Auto Network Re-Connection must be enabled in order to use this function.

Fast Flush: When enabled, the driver flushes only the local buffer on the host for a Win32 PurgeComm() function call. When disabled, both local and remote buffers are flushed. If your application uses PurgeComm() and performance seems sluggish, try enabling Fast Flush.

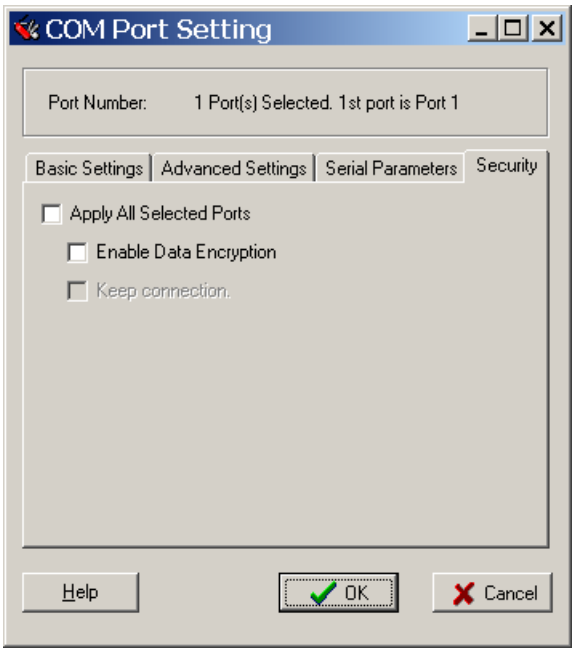
Ignore TX Purge

Applications can use the Win32 API PurgeComm to clear the output buffer. Outstanding overlapping write operations will be terminated. Select the **Ignore TX Purge** checkbox to ignore the effect on output data.

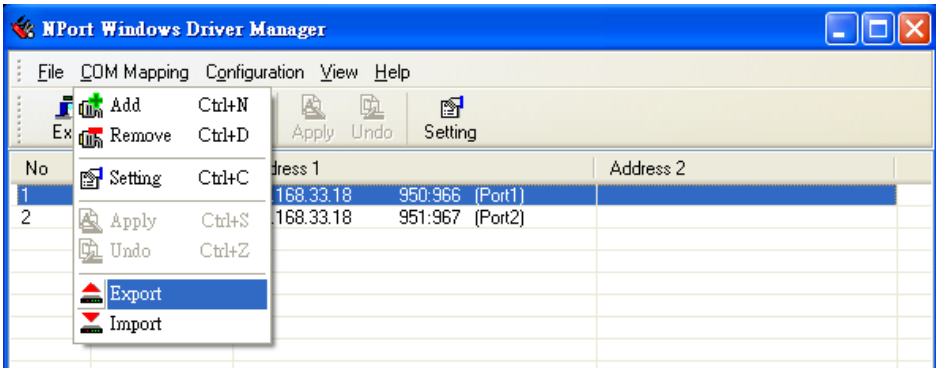
4. On the **Serial Parameters** tab, specify the communication settings that the host will use when opening the COM port.



5. On the **Security** tab, select the **Enable Data Encryption** option to enable data to be encrypted when transmitted over the COM ports. After selecting the encryption option, select the **Keep connection** option to start encrypting COM port communications immediately without restarting the COM ports. This may speed up opening and closing of the COM port for your host, but it also causes your host to tie up the NPort serial port so other hosts cannot use it.



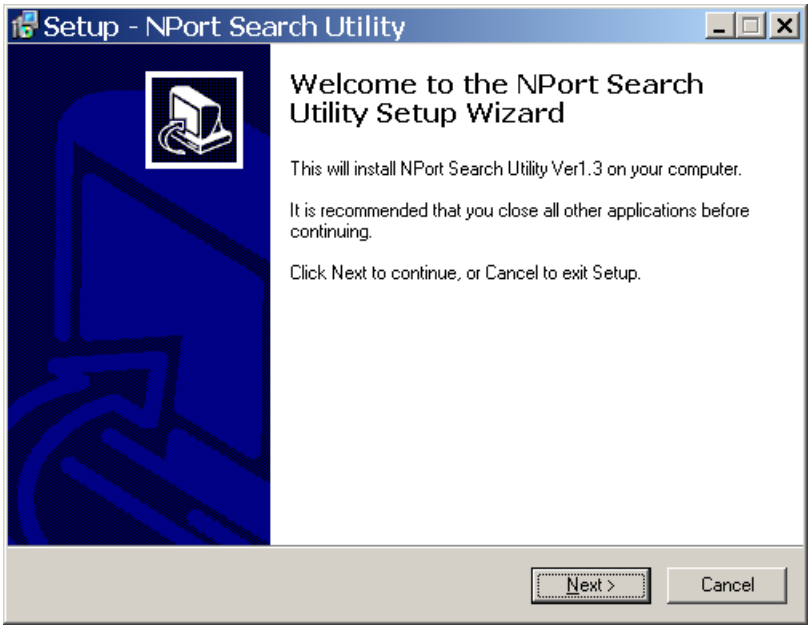
6. Click **[OK]** when you have finished configuring the COM port
7. To save all COM mapping settings to a text file, select **Export** in the context menu. After the settings have been exported to a file, they can be imported on another host.



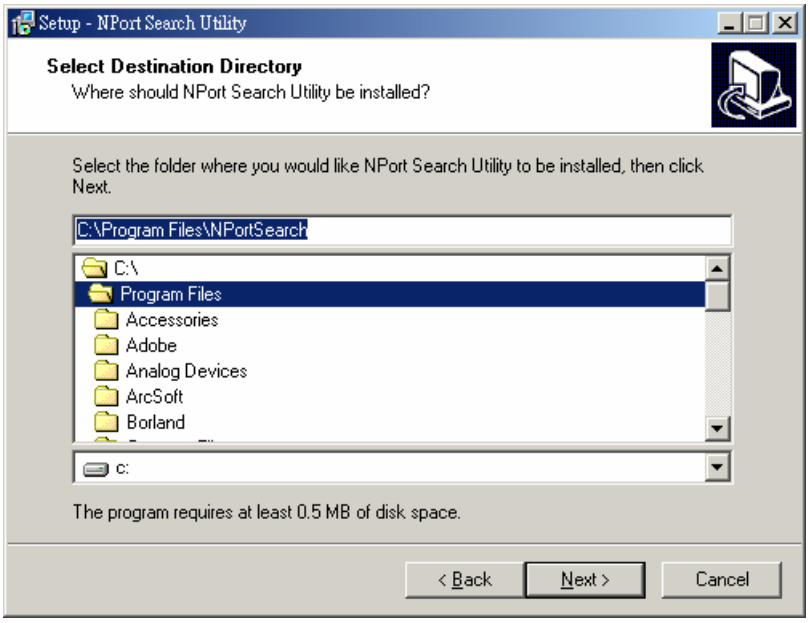
NPort Search Utility

Installing NPort Search Utility

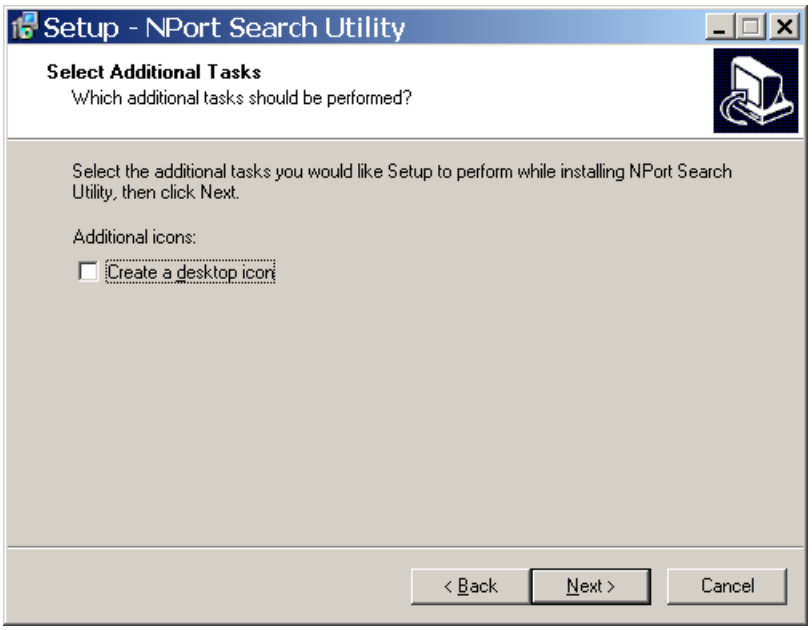
1. The main installation window will open when you insert the Document & Software CD. Click **[INSTALL UTILITY]** to proceed. Once the program starts running, click **[Yes]** to proceed.
2. The installation wizard will open. Click **[Next]** to proceed.


Setup - NPort Search Utility
Welcome to the NPort Search Utility Setup Wizard
This will install NPort Search Utility Ver1.3 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

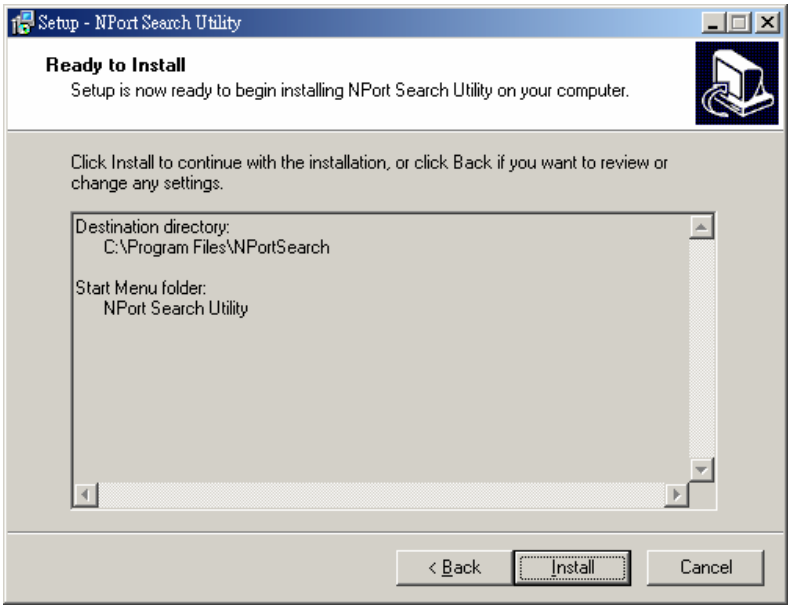
3. Select a destination directory and click **[Next]** to proceed.



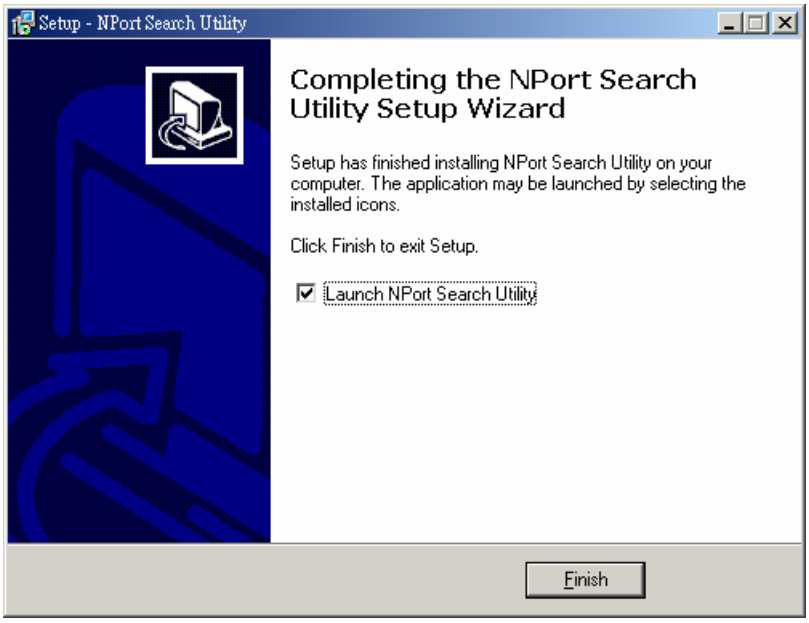
4. Indicate if you wish to create a desktop icon and click **[Next]** to proceed.


Setup - NPort Search Utility
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing NPort Search Utility, then click Next.
Additional icons:
Create a desktop icon
< Back
Next >
Cancel

5. Verify the installation parameters and click **Install** to proceed.


Setup - NPort Search Utility
Ready to Install
Setup is now ready to begin installing NPort Search Utility on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination directory:
C:\Program Files\NPortSearch
Start Menu folder:
NPort Search Utility
< Back
Install
Cancel

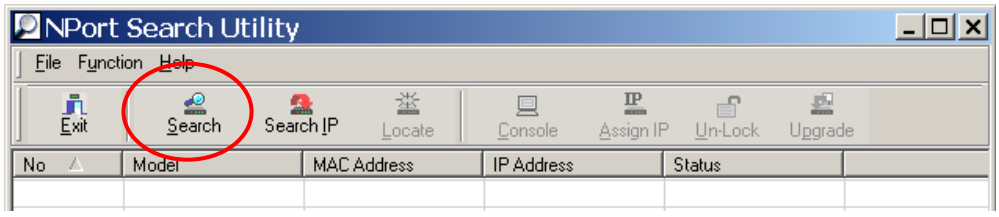
6. The wizard will begin installing the files. After the files have been installed, click **[Finish]** to complete the installation.


Setup - NPort Search Utility
Completing the NPort Search Utility Setup Wizard
Setup has finished installing NPort Search Utility on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch NPort Search Utility
Finish

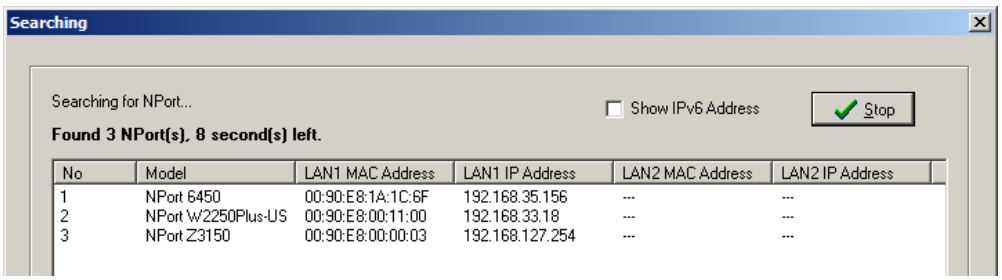
Finding NPort Device Servers on Network

You can use **NPort Search Utility** to look up or change the IP address of any NPort device servers on the network. Since the utility searches by MAC address rather than IP address, all NPort units that are connect to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

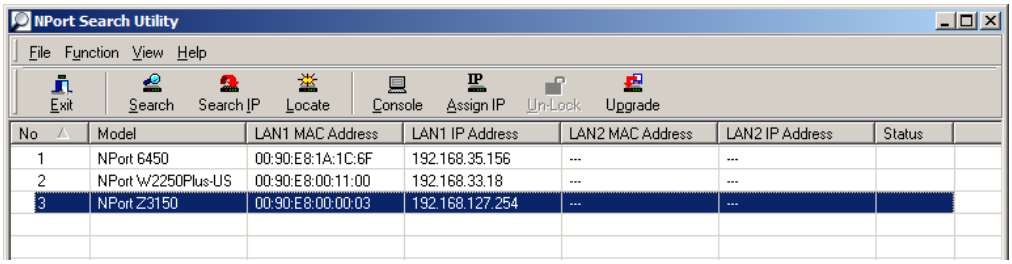
1. In **NPort Search Utilit**y, click **[Search]** on the main toolbar.



2. The utility will being searching for NPort device servers.

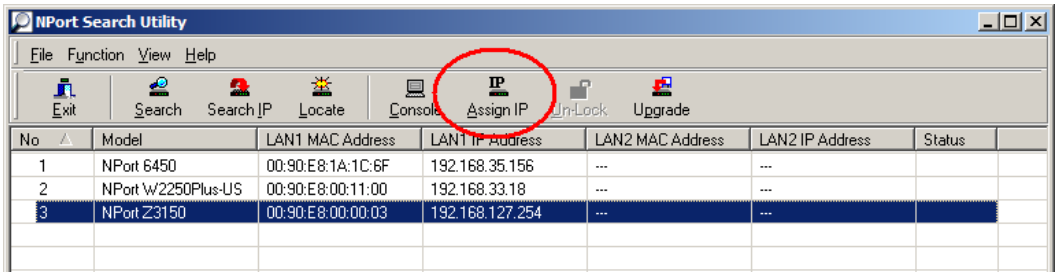


3. When the search is complete, NPort units that were found will be listed in the main window.

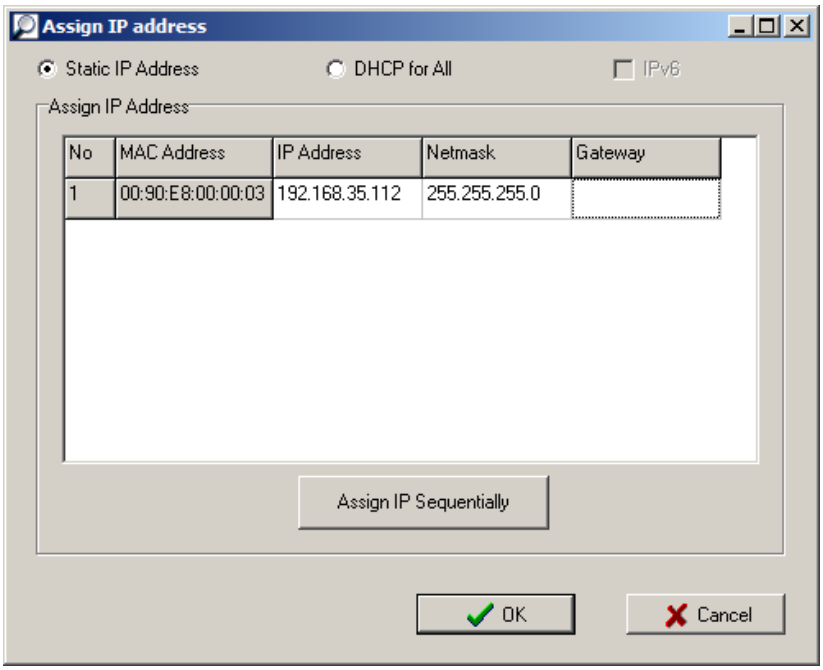


Modifying NPort IP Addresses

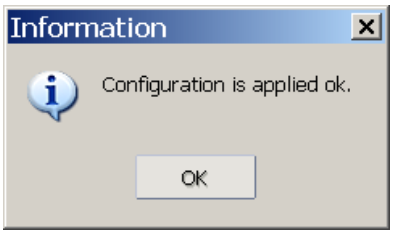
1. Once NPort Search Utility has found NPort device servers on the LAN, you can modify any unit's IP address. Select the desired NPort in the main window and click **[Assign IP]** on the main toolbar. This will modify the IP address for the active network connection (LAN or WLAN).



2. Enter the new IP address and netmask. If multiple units were selected, you may assign addresses sequentially by clicking **[Assign IP Sequentially]**. Click **[OK]** to proceed.

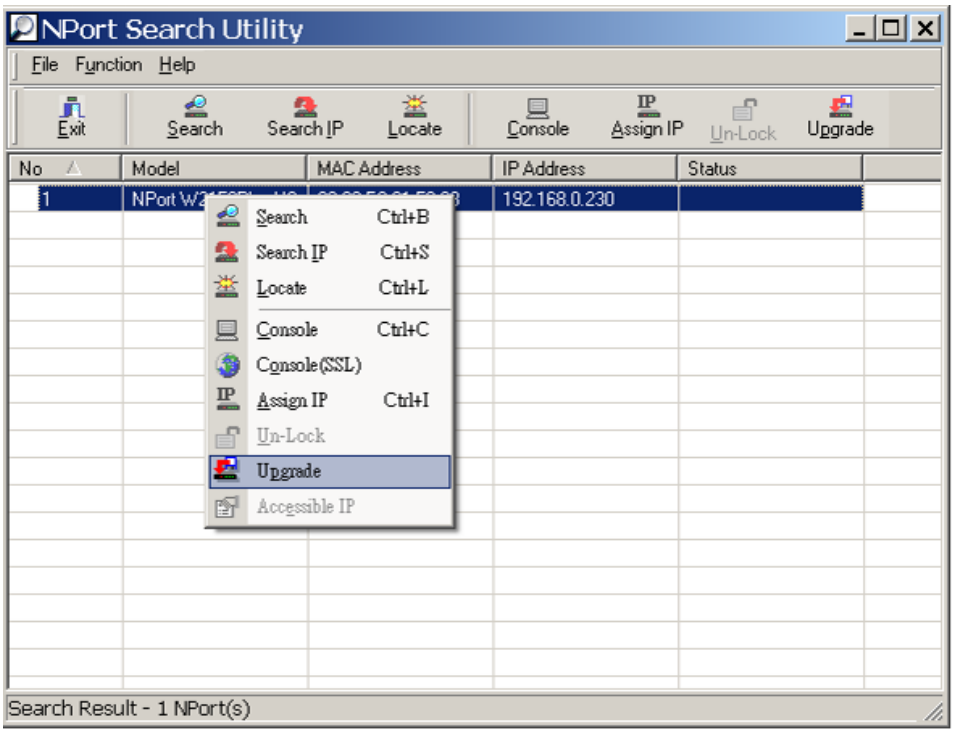


3. The selected NPort will be restarted by NPort Search Utility with the new IP address.

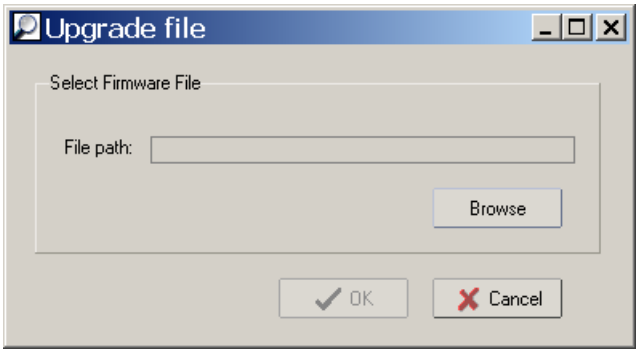


Upgrading NPort Firmware

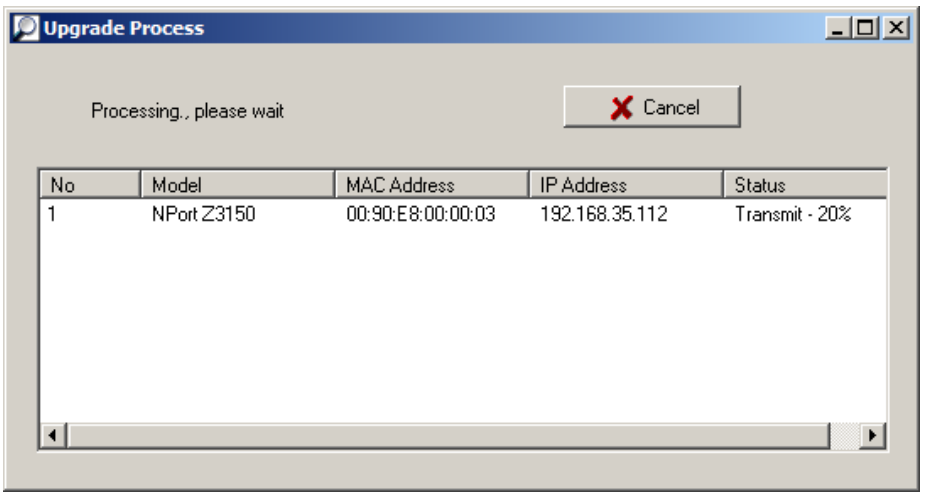
1. Once NPort Search Utility has found NPort device servers on the LAN, you can upgrade any unit's firmware. Right-click the desired NPort in the main window and select **Upgrade**.



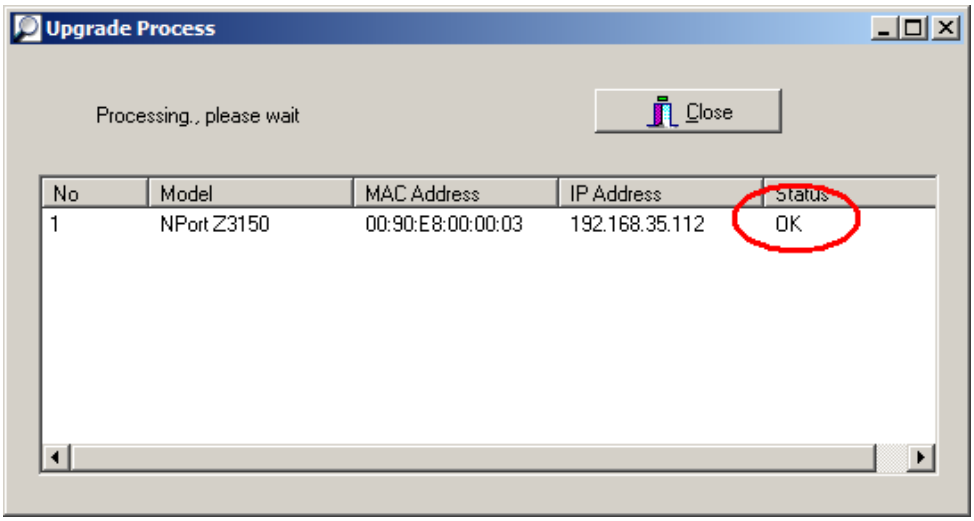
2. Select the new firmware file and click **[OK]** to proceed. To obtain the latest firmware for the NPort Z3150, visit www.moxa.com.



3. The utility will begin upgrading the firmware for the selected unit. Do not disconnect or power off the unit while the firmware is being upgraded.



4. When the displayed status is "OK", click **[Close]** to complete the process.



ATTENTION

NPort Search Utility supports upgrading the firmware of multiple units simultaneously, if each unit is the same model. Hold down the **CTRL** to add additional units to your selection; hold down the **SHIFT** key to select a block of units.

Linux Real TTY Drivers

Real TTY driver are provided that will map Linux host TTY ports to NPort serial ports. Once the mapping has been set up, Linux users and applications can connect to a serial port as if it were a local TTY port. These drivers have been designed and tested for the majority of Linux distributions, including Linux kernel version 2.4.x, 2.6.x, and 3.x. Please check http://www.moxa.com for the latest Linux kernel support.

Basic Steps

Follow these instructions to map a TTY port to a NPort serial port:

1. Install the NPort device server and set the target device port to Real COM mode.
2. Install the Real TTY driver files on the Linux host.
3. Map the host's TTY port to the target device port on the NPort.

Installing Linux Real TTY Driver Files

Before proceeding with the software installation, make sure you have completed the NPort device server has been installed and configured correctly. Note that the default LAN IP address for the NPort is **192.168.126.254**, whereas the default WLAN IP address is **192.168.127.254**.

ATTENTION

The target serial port must be operating in Real COM mode in order to map TTY ports.

1. Obtain the driver file from the Document and Software CD, or from http://www.moxa.com.
2. Log in to the console as a super user (root).
3. Execute **cd** / to go to the root directory.
4. Copy the driver file **npreal2xx.tgz** to the / directory.

5. Execute **tar xvfz npreal2xx.tgz** to extract all files into the system.
6. Execute **/tmp/moxa/mxinst**. (For RedHat AS/ES/WS and Fedora Core1, execute "# **/tmp/moxa/mxinst SP1**".) The shell script will install the driver files automatically.
7. After installing the driver, you will be able to see several files in the **/usr/lib/npreal2/driver** folder:

   mxaddsvr (add server, map TTY port)
   mxdelsvr (delete server, undo TTY port mapping)
   mxloadsvr (reload server)
   mxmknod (create device node/TTY port)
   mxrmnod (remove device node/TTY port)
   mxuninst (remove TTYport and driver files)

   At this point, you may map the TTY port to the NPort serial port.

Mapping TTY Ports

Make sure that you set the operation mode of the desired NPort serial port to Real COM mode. After logging in as a super user, enter the directory **/usr/lib/npreal2/driver** and then execute **mxaddsvr** to map the target NPort serial port to the host TTY ports. The syntax of **mxaddsvr** is as follows:

mxaddsvr [*NPort IP Address*] [*Total Ports*] ([*Data port*] [*Cmd port*])

The **mxaddsvr** command performs the following actions:

1. Modify npreal2d.cf.
2. Create TTY ports in directory /dev with major and minor number configured in npreal2d.cf.
3. Restart the driver.

Mapping TTY ports automatically

To map TTY ports automatically, you may execute **mxaddsvr** with just the IP address and number of ports, as in the following example:

 # cd /usr/lib/npreal2/driver
 # ./mxaddsvr 192.168.3.4 16

In this example, 16 TTY ports will be added, all with IP 192.168.3.4, with data ports from 950 to 965 and command ports from 966 to 981.

Mapping TTY ports manually

To map TTY ports manually, you may execute **mxaddsvr** and manually specify the data and command ports, as in the following example:

 # cd /usr/lib/npreal2/driver
 # ./mxaddsvr 192.168.3.4 16 4001 966

In this example, 16 TTY ports will be added, all with IP 192.168.3.4, with data ports from 4001 to 4016 and command ports from 966 to 981.

Removing Mapped TTY Ports

After logging in as root, enter the directory **/usr/lib/npreal2/driver** and then execute **mxdelsvr** to delete a server. The syntax of mxdelsvr is:

mxdelsvr [*IP Address*]

Example:

 # cd /usr/lib/npreal2/driver
 # ./mxdelsvr 192.168.3.4

The following actions are performed when executing **mxdelsvr**:

1. Modify npreal2d.cf.
2. Remove the relevant TTY ports in directory /dev.
3. Restart the driver.

If the IP address is not provided in the command line, the program will list the installed servers and total ports on the screen. You will need to choose a server from the list for deletion.

Removing Linux Driver Files

A utility is included that will remove all driver files, mapped TTY ports, and unload the driver. Enter the directory **/usr/lib/npreal2/driver** and execute **mxuninst** to uninstall the driver. This program will perform the following actions:

1. Unload the driver.
2. Delete all files and directories in /usr/lib/npreal2.
3. Delete directory /usr/lib/npreal2.
4. Modify the system initializing script file.

UNIX Fixed TTY Drivers

A fixed TTY driver is provided that will map UNIX host TTY ports to NPort serial ports. Once the mapping has been set up, UNIX users and applications can connect to an NPort serial port as if it were a local TTY port. This driver has been designed and tested for the majority of UNIX systems. Please check http://www.moxa.com for the latest UNIX systems support.

Installing the UNIX Driver

1. Log in to UNIX and create a directory for the MOXA TTY. To create a directory named **/usr/etc**, execute the command:

   # mkdir –p /usr/etc

2. Copy **moxattyd.tar** to the directory you created. For the /usr/etc directory, you would execute the following commands:

   # cp moxattyd.tar /usr/etc
   # cd /usr/etc

3. Extract the source files from the tar file by executing the command:

   # tar xvf moxattyd.tar

   The following files will be extracted:

   README.TXT
   moxattyd.c --- source code
   moxattyd.cf --- an empty configuration file
   Makefile --- makefile
   VERSION.TXT --- fixed TTY driver version
   FAQ.TXT

4. Compile and link.

   For SCO UNIX:
   # make sco

   For UnixWare 7:
   # make svr5

   For UnixWare 2.1.x, SVR4.2:
   # make svr42

Configuring the UNIX Driver

Modify the configuration:

The configuration used by **moxattyd** is defined in the text file **moxattyd.cf**, which is in the same directory. You may use vi or any text editor to modify the file, as follows:

ttyp1 192.168.1.1 950

You can refer to **moxattyd.cf** for detailed descriptions of the various configuration parameters. Please note that "Device Name" depends on the OS. See the Device Naming Rule section in README.TXT for more information.

To start the moxattyd daemon after system bootup, add an entry into **/etc/inittab** using the TTY name you defined in **moxattyd.cf**, as in the following example:

ts:2:respawn:/usr/etc/moxattyd/moxattyd –t 1

Device naming rule

For UnixWare 7, UnixWare 2.1.x, and SVR4.2, use:

pts/[*n*]

For all other UNIX operating systems, use:

ttyp[*n*]

The value of [n] should be equal or larger than 11 in order to prevent conflicts with the device names of functional keys in some UNIX systems.

Starting moxattyd

Execute the command **init q** or reboot your UNIX operating system.

Adding an additional server

Modify the text file **moxattyd.cf** to add an additional server. User may use vi or any text editor to modify the file. For more configuration information, refer to **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.

Find the process ID (PID) of the **moxattyd**.

 # ps -ef | grep moxattyd

Update the configuration of **moxattyd**.

 # kill -USR1 [*PID*]
(e.g., if moxattyd PID = 404, **kill -USR1 404**)

This completes the process of adding an additional server.

A

SNMP Agents with MIB II & RS-232-Like Groups

The NPort has built-in SNMP (Simple Network Management Protocol) agent software that supports SNMP Trap, RFC1317 RS-232 like groups and RFC 1213 MIB-II. The following table lists the standard MIB-II groups, as well as the variable implementation for the NPort.

The following topics are covered in this appendix:

- **RFC1213 MIB-II Supported SNMP Variables**
  - System MIB
  - Interfaces MIB
  - IP MIB
  - ICMP MIB
  - UDP MIB
  - Address Translation
  - TCP MIB
  - SNMP MIB
- **RFC1317: RS-232 MIB Objects**
  - Generic RS-232-like Group
  - RS-232-like General Port Table
  - RS-232-like Asynchronous Port Group
  - The Input Signal Table
  - The Output Signal Table

RFC1213 MIB-II Supported SNMP Variables

System MIB

SysDescr
SysObjectID
SysUpTime
SysContact
SysName
SysLocation
SysServices

Interfaces MIB

itNumber
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQLen
ifSpecific

IP MIB

ipForwarding
ipDefaultTTL
ipInreceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipInUnknownProtos
ipInDiscards
ipInDelivers
ipOutRequests
ipOutDiscards
ipOutNoRoutes
ipReasmTimeout
ipReasmReqds
ipReasmOKs
ipReasmFails
ipFragOKs
ipFragFails
ipFragCreates
ipAdEntAddr
ipAdEntIfIndex
ipAdEntNetMask
ipAdEntBcastAddr
ipAdEntReasmMaxSize
IpNetToMediaIfIndex
IpNetToMediaPhysAddress
IpNetToMediaNetAddress
IpNetToMediaType
IpRoutingDiscards

ICMP MIB

IcmpInMsgs
IcmpInErrors
IcmpInDestUnreachs
IcmpInTimeExcds
IcmpInParmProbs
IcmpInSrcQuenchs
IcmpInRedirects
IcmpInEchos
IcmpInEchoReps
IcmpInTimestamps
IcmpTimestampReps
IcmpInAddrMasks
IcmpOutMsgs
IcmpOutErrors
IcmpOutDestUnreachs
IcmpOutTimeExcds
IcmpOutParmProbs
IcmpOutSrcQuenchs
IcmpOutRedirects
IcmpOutEchos
IcmpOutEchoReps
IcmpOutTimestamps
IcmpOutTimestampReps
IcmpOutAddrMasks
IcmpOutAddrMaskReps

UDP MIB

UdpInDatagrams
UdpNoPorts
UdpInErrors
UdpOutDatagrams
UdpLocalAddress
UdpLocalPort

Address Translation

AtIfIndex
AtNetAddress
AtPhysAddress

TCP MIB

tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens
tcpAttempFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnState
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts

SNMP MIB

snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps

RFC1317: RS-232 MIB Objects

Generic RS-232-like Group

rs232Number

RS-232-like General Port Table

rs232PortTable
rs232PortEntry
rs232PortIndex
rs232PortType
rs232PortInSigNumber
rs232PortOutSigNumber
rs232PortInSpeed
rs232PortOutSpeed

RS-232-like Asynchronous Port Group

rs232AsyncPortTable
rs232AsyncPortEntry
rs232AsyncPortIndex
rs232AsyncPortBits
rs232AsyncPortStopBits
rs232AsyncPortParity

The Input Signal Table

rs232InSigTable
rs232InSigEntry
rs232InSigPortIndex
rs232InSigName
rs232InSigState

The Output Signal Table

rs232OutSigTable	rs232OutSigPortIndex	rs232OutSigState
rs232OutSigEntry	rs232OutSigName	

B

ZigBee Introduction

ZigBee is a standard that defines a set of communication protocols for low-data-rate, short-range wireless networking. ZigBee-based wireless devices operate in 868 MHz, 915 MHz, and 2.4 GHz frequency bands. The maximum data rate is 250 K bits per second. ZigBee is utilized mainly for battery-powered applications where low data rate, low cost, and long battery life are main concerns. In many ZigBee applications, the total time the wireless device is engaged in any type of activity is very limited; the device spends most of its time in a power-saving mode, also known as sleep mode . As a result, ZigBee-enabled devices are capable of being operational for several years before their batteries need to be replaced.

One application of ZigBee is in-home patient monitoring. A patient's blood pressure and heart rate, for example, can be measured by wearable devices. The patient wears a ZigBee device that interfaces with a sensor that gathers health-related information, such as blood pressure, on a periodic basis. Then the data is wirelessly transmitted to a local server, such as a personal computer inside the patient's home, where initial analysis is performed. Finally, the vital information is sent to the patient's nurse or physician via the Internet for further analysis.

The following topics are covered in this appendix:

- **Device Type**
- **Network Topology**

Device Type

The ZigBee standard uses slightly different terminology:

ZigBee coordinator: an IEEE 802.15.4-2003 PAN coordinator.

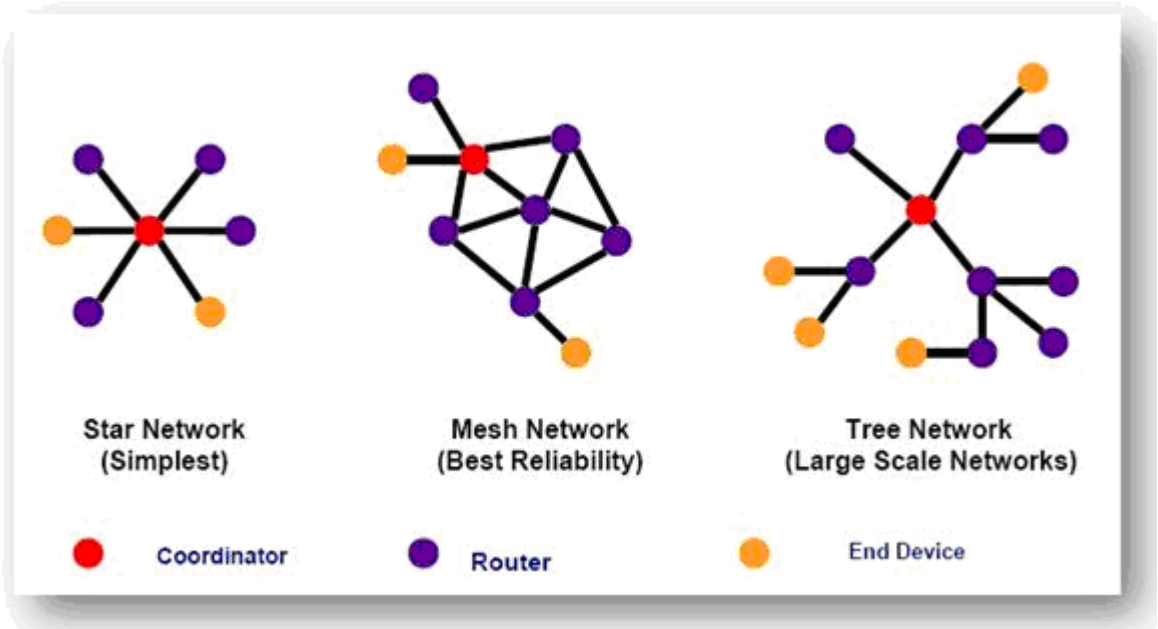
ZigBee end device: an IEEE 802.15.4-2003 RFD or FFD participating in a ZigBee network, which is neither the ZigBee coordinator nor a ZigBee router.

ZigBee router: an IEEE 802.15.4-2003 FFD participating in a ZigBee network, which is not the ZigBee coordinator but may act as an IEEE 802.15.4-2003 coordinator within its personal operating space, that is capable of routing messages between devices and upporting associations.

Network Topology

The ZigBee network layer (NWK) supports star, tree, and mesh topologies. In a star topology, the network is controlled by one single device called the ZigBee coordinator. The ZigBee coordinator is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator. In mesh and tree topologies, the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters, but the network may be extended through the use of ZigBee routers. In tree networks, routers move data and control messages through the network using a hierarchical routing strategy. Tree networks may employ beacon-oriented communication as described in the IEEE 802.15.4-2003 specification. Mesh networks allow full peer-to-peer communication. ZigBee routers in mesh networks do not currently emit regular IEEE 802.15.4-2003 beacons. This specification describes only intra-PAN networks, that is, networks in which communications begin and terminate within the same network.

In the star topology, every device in the network can communicate only with the PAN coordinator. A typical scenario in a star network formation is that an device, programmed to be a PAN coordinator, is activated and starts establishing its network. The first thing this PAN coordinator does is select a unique PAN identifier that is not used by any other network in its radio sphere of influence —the region around the device in which its radio can successfully communicate with other radios. In other words, it ensures that the PAN identifier is not used by any other nearby network.



In a Mesh topology each device can communicate directly with any other device if the devices are placed close enough together to establish a successful communication link. Any devices in a peer-to-peer network can play the role of the PAN coordinator. One way to decide which device will be the PAN coordinator is to pick the first device that starts communicating as the PAN coordinator. In a peer-to-peer network, all the devices that participate in relaying the messages are devices because devices are not capable of relaying the messages. However, an device can be part of the network and communicate only with one particular device (a coordinator or a router) in the network.

ZigBee supports a tree topology. In this case, a ZigBee coordinator (PAN coordinator) establishes the initial network. ZigBee routers form the branches and relay the messages. ZigBee end devices act as leaves of the tree and do not participate in message routing. ZigBee routers can grow the network beyond the initial network established by the ZigBee coordinator.

Note: this section refers to the book: "ZigBee Wireless Networks and Transceivers"

C

Well Known Port Numbers

Listed below are Well Known Port Numbers that may cause network problems if they are assigned to an NPort serial port. Refer to RFC 1700 for Well Known Port Numbers or refer to the following introduction from IANA.

The port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports.

- **Well Known Ports** range from 0 through 1023.
- **Registered Ports** range from 1024 through 49151.
- **Dynamic** and/or **Private Ports** range from 49152 through 65535.

The Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the well-known port numbers. For more details, please visit the IANA website at http://www.iana.org/assignments/port-numbers.

TCP Socket	Application Service
0	reserved
1	TCP Port Service Multiplexor
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP CONTROL port
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (Login)
53	Domain Name Server (domain)
79	Finger protocol (Finger)
80	World Wide Web HTTP
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use

UDP Socket	Application Service
0	reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (Login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TETP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web HTTP
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	(Simple Network Mail Protocol (SNMP)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

D

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference received, including interference that may cause undesired operation.

E

FCC Warning Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, when installing and/or operating this equipment, you should maintain a minimum distance of 20 cm between the transmitter and your body. Use only the supplied antenna. Unauthorized antennae, modifications, or attachments could damage the transmitter and may violate FCC regulations.

NOTE Please refer to the book: "ZigBee Wireless Networks and Transceivers"